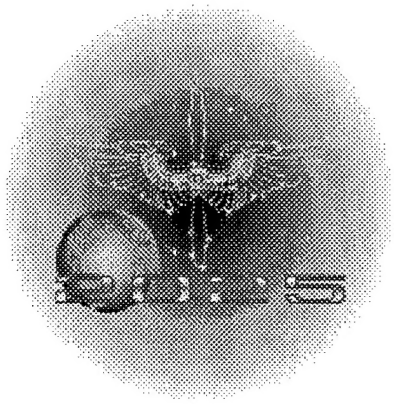
Information Operations:
A New War-Fighting Capability



A Research Paper
Presented To

Air Force *2025*

by

LTC William B. Osborne (USA)
Maj Scott A. Bethel
Maj Nolen R. Chew
Maj Philip M. Nostrand
Maj YuLin G. Whitehead

August 1996

01 DECEMBER 1997

POC: AIR WAR COLLEGE.
AIR COMMAND AND STAFF COLLEGE
MAXWELL AFB, AL 36112

Disclaimer

2025 is a study designed to comply with a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies the United States will require to remain the dominant air and space force in the future. Presented on 17 June 1996, this report was produced in the Department of Defense school environment of academic freedom and in the interest of advancing concepts related to national defense. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States government.

This report contains fictional representations of future situations/scenarios. Any similarities to real people or events, other than those specifically cited, are unintentional and are for purposes of illustration only.

This publication has been reviewed by security and policy review authorities, is unclassified, and is cleared for public release.

Contents

Chapter *Page*

Appendix *Page*

Illustrations

Tables

Preface

You see things; and say "Why?" But I dream of things that never were; and I say; "Why not?"

—George Bernard Shaw
Back to Methuselah, part 1, act 1

This project envisions war-fighting capabilities that will enable military members to prosecute operations effectively in support of vital national strategic interests determined by US political leaders. Our efforts stem from a genuine concern to improve the tools to assist commanders in an age of exponential growth in available information. But, this vision goes beyond just giving commanders useful information; it aims to empower them with the ability to leverage information to conduct warfare.

We undertook this effort knowing that some readers would find it a challenge to project their thoughts out into the next millennium to 2025. Nevertheless, we encourage our readers to "double leap" into 2025 and share our excitement in the concept's potential to keep the US military as the best military in the world.

We appreciate Air University's pushing us beyond the safe envelope of thinking and planning the future. Without exception, we received impressive assistance from advisors, instructors, guest speakers, and peers. Finally, our spouses supported and encouraged us when we needed it most—when naysayers doubted our "out-of-box" visions.

Never again will we say "that can't be done." Others may see the impossible, but we will determine "how?"

Executive Summary

> *The affirming characteristic of Alexander the Great's genius as a general and leader was "the startling rapidity with which he always acted. . . . Time was his constant ally; he capitalized every moment, never pondered on it, and thereby achieved his end before others had settled on their means."*
>
> —J.F.C. Fuller
> *The Generalship of Alexander the Great*

In its most basic form, commanders have always performed the functions of observe, orient, decide, and act (OODA Loop) to prosecute military operations.[1] As with Alexander the Great, history shows the military commander who best analyzes, decides, and controls the speed of the engagement prevails in nearly every conflict. To master the OODA Loop, military leaders have pushed technology to obtain more information.[2] Ironically, this situation now leads to the requirement to solve two fundamental challenges if the United States expects to maintain air and space dominance in 2025. First, the proliferation of unintegrated military war-fighting architectures gives the commander potentially conflicting perspectives of the battlespace.[3] Second, the explosion of available information creates an environment of mental overload leading to flawed decision making. Failure to master these challenges critically weakens the military instrument of power. This paper presents a solution to these challenges by confronting commanders as they employ future airpower forces.

Regarding the first challenge, the large number of specialized war-fighting architectures makes information integration supporting overall coordination and control more important and more difficult. Simultaneously, the speed and the range of modern weapons drastically reduces the time commanders have to integrate conflicting information and decide on a course of action.

The second challenge is to harness the information explosion to combat mental overload, thus improving decision making. Recent exercises reveal an alarming number of unread messages because of information overload.[4] As the quantity of data rises, the difficulty of preparing and interpreting it for decision making grows. Traditionally, the military attempted to solve this problem by increasing the number of

communications nodes. These past solutions only injected additional inputs and information without improving decision-making capability.

The optimum solution must integrate the functions within the OODA Loop and allow the commander to control the momentum of the cycle. This paper describes how a system, called the Cyber Situation, can do just that, thus optimizing commanders' ability to operate air and space systems. The Cyber Situation enables commanders and decision makers to have in-time access to the battlespace, characterize the nature of the engagement, determine the calculated probabilities of success from the various authorized lethal or nonlethal options, decide what to do, employ the weapons chosen, and receive in-time feedback on the result of the engagement.

The Cyber Situation system includes five major components. First, all-source information collectors will transmit raw data to the Information Integration Center (IIC), as discussed below. Second, archival databases, linked to the IIC, will be used for historical analyses to fill information gaps if the data is not available for collection. Third, the IIC, an integrated and interconnected constellation of "smart" satellites will analyze, correlate, fuse, and deconflict all relayed data. Fourth, implanted microscopic chips link users to the IIC and create computer-generated mental visualizations.[5] The visualization encompasses the individual and allows the user to place himself into the selected battlespace. Fifth, lethal and nonlethal weapons will be linked to the IIC, allowing authorized users to employ them from the Cyber Situation.

Implied in the Cyber Situation are five key technologies evolving on separate paths that will synergize by 2025 to achieve this goal. They include collection platforms, communications infrastructure, computing power, intelligent software, and human systems and biotechnology. Most of these technologies will evolve through the commercial community, but the military must focus research and development efforts on biological and computational intelligent software and biotechnology breakthroughs to allow mental visualization.

Once realized, these new capabilities will give commanders a new way to prosecute warfare. New technology alone does not revolutionize warfare. Rather, technology's impact on systems evolution, operational tactics, and organizational structure is its true advantage.[6] This fuels necessary and complementary changes in doctrine and organizational structure.

Organizations and doctrine will need to adapt to a streamlined, decentralized environment. The traditional emphasis on command and control will give way to an emphasis on consultation and control. This organizational structure permits the Cyber Situation to operate at maximum efficiency. It also allows commander's at all levels to operate with a greater degree of latitude and autonomy as part of an integrated joint operation—a truly combined arms.

Airpower in 2025 must make optimum use of information technology to operate inside an opponent's decision cycle. This requires unequivocal dominance of cyberspace. In addition to enabling all military pursuits, information-related activities will transcend all air and space operations.

To be sure, the Cyber Situation proposed in this paper certainly will not eliminate all the command problems facing airpower forces in 2025. However, it may well shed light on the main factors involved and indicate the direction any reform efforts should move. The challenge now is for airpower strategists to develop the war-fighting doctrine to turn the vision of a true battlespace execution capability into reality.

Notes

[1] Maj David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell AFB, Ala.: Air University Press, February 1995), 16.

[2] Examples of technology push to obtain more information range from observation balloons to surveillance and reconnaissance aircraft and satellites.

[3] "War-fighting architectures" encompass the entire spectrum of systems (information collection, processing, dissemination; command and control; and offensive and defensive weapons systems) to support military operations.

[4] A senior US Department of Defense policymaker lecture given to the 1996 Air Command and Staff College under the promise of nonattribution. The individual stated that during a 1995 Joint Task Force exercise, three thousand of the thirty thousand messages used in the exercise were never opened nor viewed by anyone because of information overload.

[5] 2025 Concept, No. 900702, "Implanted Tactical Information Display," 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996).

[6] Andrew F. Krepinevich, Jr., *War Theory*, vol. 3, *The Military-Technical Revolution: A Preliminary Assessment* (Maxwell AFB, Ala.: Air University Press, September 1995), 163-64.

Chapter 1

Introduction

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

—Giulio Douhet
The Command of the Air

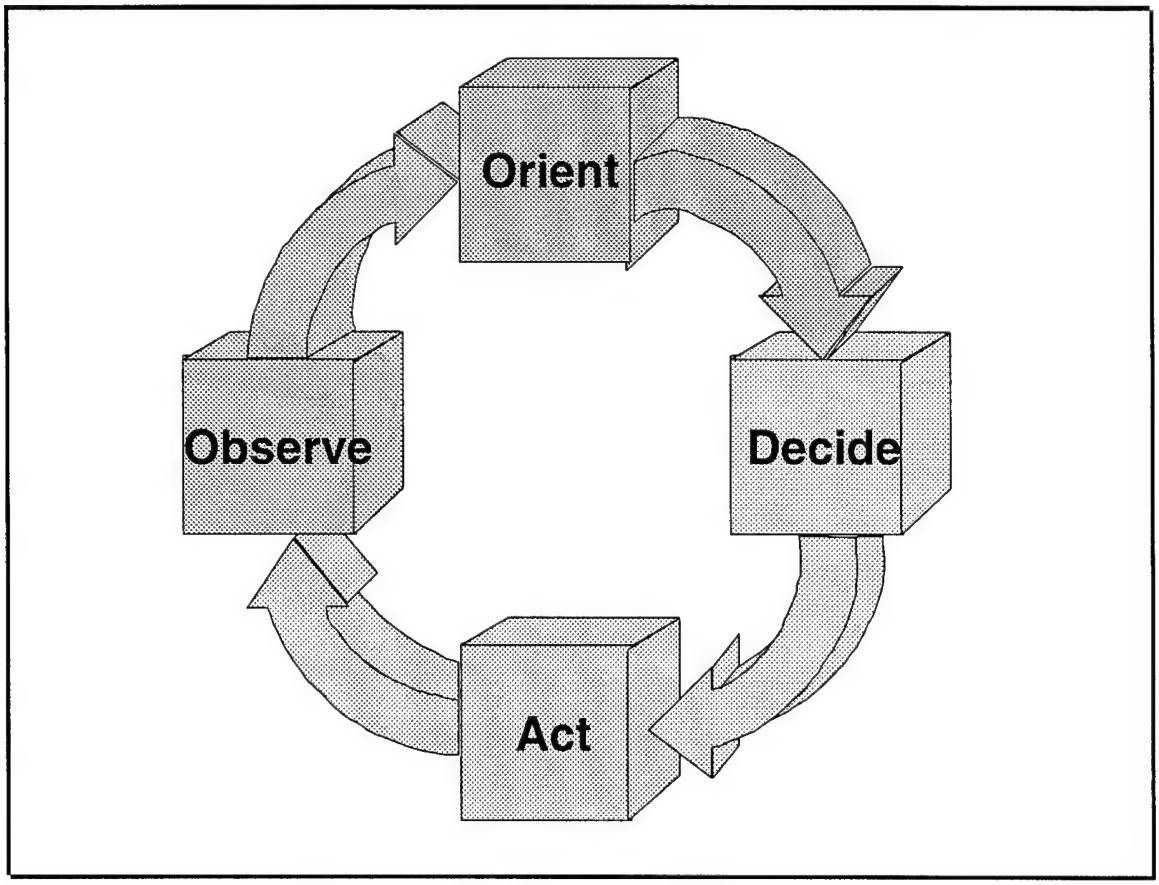
Victory smiles upon those who change the character of war to their advantage, not upon those who merely anticipate the change or wait to adapt themselves after the changes occurs.

—Joseph A. Engelbrecht, Jr.
AIR FORCE ***2025*** Research Director

The Challenges

History clearly shows the military commander who best analyzes, decides, and controls the speed of the engagement prevails in nearly every conflict. In the simplest form of conflict, commanders have traditionally performed the functions of observe, orient, decide, and act (OODA Loop) to prosecute military operations (fig. 1-1).[1] To master the OODA Loop, military leaders have pushed technology to obtain more information. This push attempts to achieve the core capability of information dominance that "is the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same."[2] The need for information dominance is vital, because "the emergence of the information and technology age presents new challenges to US strategy even as it offers extraordinary chances to build a better future."[3] In today's world, satellite surveillance and reconnaissance technology provide a unique view of those challenges from

the ultimate high ground. Extensive communications links and superior data-processing capabilities allow improved distribution of this information.



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 1-1. OODA Loop

Ironically, this situation now leads to two fundamental challenges if the United States expects to continue its dominance of air and space in 2025. First, the proliferation of unintegrated military war-fighting architectures gives commanders potentially conflicting perspectives of the battlespace.[4] Second, the explosion of available information creates an environment of mental overload leading to flawed decision making. Failure to master these challenges critically weakens the military instrument of power.

The two challenges have resulted in a scenario not unfamiliar to current military operations. Commanders *observe* after waiting for collection assets to assimilate data and analysts to process and interpret the information; *orient* based upon inputs and further interpretations from their staffs that may be conflicting or, worst yet, wrong; *decide* with generally incomplete, imperfect, and possibly biased

information; and *act* without first being able to forecast the probability of success of the action or having direct and immediate access to employment tools. Gaps and weaknesses in each step widen and exacerbate as each cycle begins anew.

In 2025 operating near the speed of light will be a common feature of military engagements. Future architectures envision a new array of ground- and space-based sensors, uninhabited combat aerial vehicles (UCAV), and missile defense technology which will take advantage of developing directed energy capabilities. If a kill mechanism operates at the same speed as the flow of information, a defender cannot possess the requisite time to observe the attack, orient himself, decide how to respond, and act on that decision. As a result, the attacker would get inside the defender's OODA Loop, destroying the ability to conduct an active defense.

This paper proposes a solution to these challenges confronting commanders employing future airpower. The optimum solution should integrate the functions within the OODA Loop and allow the commander to control the momentum of the cycle. Further, the solution should enable commanders and decision makers to have in-time access to the battlespace, characterize the nature of the engagement, determine the calculated probabilities of success from the various lethal or nonlethal options authorized, decide what to do, employ the weapons chosen, and receive in-time feedback on the result of the engagement.[5] Simply stated, the solution should go beyond just giving commanders useful information; it should empower them with the ability to leverage information to conduct warfare.

Assumptions

For planning to achieve information dominance, the following assumptions are plausible for 2025:

1. Information is power. Hence, the high ground of the future will be information dominance.[6]

2. Expect continued explosion in the proliferation of information.[7] The availability of information is overwhelming, and the driving issue that will contribute to success is being able to sift the "gold from the dross."[8] Accordingly, collection assets, regardless of where they are based, will be sufficiently available in 2025.

3. The site, size, and scope of future conflicts are unknown. The United States military must be prepared to fight or to conduct mobility or special operations anywhere in the world on short notice.[9]

4. The military will have to fight at long distances from the United States. In particular, some operations may be staged directly from the continental United States. These operations may endure for weeks or months in weather conditions executed both during the day and night.[10]

5. Adversary capabilities steadily will improve and will be difficult to forecast.[11] The United States must assume we will fight smart enemies who have analyzed all aspects of our military doctrine, capabilities, and operations. Further, they will develop weapon systems to attack their perceived vulnerabilities of United States military forces.

6. Military personnel strength will continue to decrease, thus placing further importance on optimizing individual performance.[12]

7. Today's principles of war will still be applicable in 2025.[13] They include the need to gain the offensive, achieve unity of command, maintain security, exploit surprise, use mass and maneuver while practicing simplicity, and employ economy of force.

The Rest of the Story

The remainder of this paper discusses the proposed solution and its implications. Chapter 2 explains the required capability by outlining the need for OODA Loop integration and momentum control. Chapters 3 and 4 take the reader through the technology evolution that synergizes in the solution called Cyber Situation. Chapter 5 discusses vulnerabilities and countermeasures. Chapter 6 outlines how the Cyber Situation functions and its implications on doctrine, tactics, organization, and force structures. Finally, chapter 7 recommends areas requiring additional research and chapter 8 offers a conclusion to this paper.

Overall, this paper focuses on the conceptual fusion of information operations. Other 2025 papers deal specifically with various aspects of information operations.[14] Furthermore, other papers focus on technologies this paper assumes will be available in 2025, including space lift, uninhibited aerial vehicles (UAV), and other lethal weapons.[15] This paper serves as the integrator of future information operations

technology—a concept that enables military commanders to observe the battlespace, analyze events, and direct forces from within a single entity.

Notes

[1] Maj David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell AFB, Ala.: Air University Press, February 1995), 16.

[2] Dr Sheila E. Widnall and Gen Ronald R. Fogelman, *Air Force Executive Guidance* (Washington, D. C.: December 1995), 2, 17. This document outlines five Air Force areas of core competency—air superiority, space superiority, global mobility, precision employment, and information dominance.

[3] William J. Clinton, *A National Security Strategy of Engagement and Enlargement* (the White House, February 1996), 1.

[4] "War-fighting architectures" encompass the entire spectrum of systems (information collection, processing, dissemination; command and control; and offensive and defensive weapons systems) to support military operations.

[5] The use of "in-time" as opposed to real-time or near-real time puts the focus on both timeliness and requirement for information. In-time access means getting information to users *in time* to perform a mission or task.

[6] Widnall and Fogelman, 16.

[7] Martin C. Libicki, *The Mesh and the Net: Speculation on Armed Conflict in a Time of Free Silicon* (Washington, D. C.: National Defense University Press, 1994), 2-3.

[8] Francis Fukuyama, RAND, Electronic Mail, subject: Dross and Gold, 27 December 1995. Used by permission of author. This electronic mail stresses the importance of "sorting the gold from the dross" because of "data deluge" and the problem of "facing too much wrong information, a phenomenon often exacerbated by new information systems."

[9] Air Force Scientific Advisory Board, *New World Vistas,* Air and Space Power for the 21st Century Volume, 15 December 1995, 5.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992, 16.

[14] Other 2025 Study research papers dealing with aspects of information operations include: Maj Cindy Norman, et al., "Man In the Chair" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); Maj Mike Tiernan et al., "In-Time Information Integration System" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); and Maj Barbara Jefts et al., "Virtual Integrated Planning and Execution Resources System: The High Ground of 2025" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996).

[15] Other 2025 Study research papers dealing with spacelift, UAVs and lethal weapons include Lt Col Bruce Carmichael et al., "DEATHSTAR 2025" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); Lt Col Henry Baird et al., "Spacelift" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); and Maj Philip Simonsen et al., "On-Orbit Support" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996).

Chapter 2

Required Capability

Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the mind of humans. That's where the battles are won.

—Col John Boyd

Information Dominance

As a new millennium approaches, information dominance should become a "blue print" for continued success as a superpower and contribute to peace particularly by adding new dimensions to deterrence.[1] Currently, information operations focuses too narrowly on the acquisition, transmission, and storage of information. Today's *Cornerstones of Information Warfare* defines military information functions (operations) as surveillance, reconnaissance, command and control, intelligence, communications, combat identification, precision navigation, and weather.[2] In 2025 the definition will likely include tools that allow military leaders to integrate seamlessly the functions of the OODA Loop and the ability to control momentum.

Speed and Accuracy of OODA Loops

Every individual operates a OODA Loop that is unique in speed and accuracy (fig. 1-1). Speed is based on the individual's mental capacity and capability to deal with information and changing environments. John Boyd asserts that one can paralyze an enemy by operating inside his OODA Loop, meaning that the individual is operating a faster cycle speed than the enemy's.[3] Accuracy is determined during the orient part

of the cycle by what information is filtered and how it is organized. Boyd considers the orientation as the most important part of the cycle because "it shapes the way we interact with the environment—hence orientation shapes the way we observe, the way we decide, the way we act."[4]

Dross Versus Gold

Increasingly, the OODA cycle time is affected by a growing deluge of information, with much of it insignificant or not applicable to the task at hand.[5] The difficulty lies in filtering out exactly the nuggets of information that are useful. Unfortunately, during combat operations, most commanders possess limited time to perform specific tasks and issue orders. Further, as increased volumes of information are input into the OODA Loop or as the rate of input increases, natural defense mechanisms tend to try to protect people.[6] A key mechanism is a "bounded rationality"[7] that allows individuals to screen out inputs prior to being overloaded or inundated so they can continue to focus on a particular task. One danger lies in the commanders screening out "golden nuggets" because they are focused elsewhere. A second danger lies in failing to recognize when new data should dictate a refocus or reorientation.

OODA Loop "Integration"

Technology, however, can integrate functions within the OODA Loop and speed up the cycle. It does this by creating decision support tools to alleviate the precarious situation that exists when crucial nuggets of information are omitted from the individual's OODA Loop. The tools, designed especially for commanders, would aid in managing military information to fit how commanders actually assess situations and issue orders.[8] The decision support tools would assist commanders to deal with inputs from different, sometimes contradictory or incremental, sources. Unfortunately, the integration tools do not currently exist. This paper proposes the development of this capability in subsequent chapters.

"Momentum Control"

Thus far, we have assumed that technology will assist the commander by increasing the speed and improving the accuracy of his OODA Loop. However, it is also possible successful military operations will require a "loosening" of the loop.[9] Specifically, technology should also allow the commander to "control momentum" of the OODA Loop. In other words, the commander must be able to control the cycle speed to allow the "modulation of both time and space" so the "impulse of strategic power is imparted at the proper moment to the objective at a critical position."[10] The final stage of employing or impulsing the strategic power must be "kept short so as to minimize the enemy's ability to avoid the onslaught or effect countermeasures."[11]

"Momentum control" is an unorthodox concept because the information age compels users to believe that faster and shorter OODA Loop cycles are the goal. However, there may be opportunities where slowing the cycle benefits the commander's operations and induces friction in the enemy's cycle. Momentum control includes the ability to operate within the desired time cycles, both by controlling friendly movement and by affecting an enemy's movement.[12] For example, a special operations soldier camouflaged to match the terrain will move relatively fast toward an enemy camp. Yet, once he is within viewing distance of the enemy, his movement slows to a minuscule rate to prevent enemy detection. The soldier has slowed his OODA Loop cycle by controlling momentum in both time and space. Another example is the strategic football coach whose team has a lead late in the fourth quarter and who employs the running game when his team is on offense. Like the soldier, the savvy coach wants to control the momentum of the battle, to slow the OODA Cycle by using time (the clock continues to tick between running plays) and space (achieving enough yards every three or four plays to get a first down) to defeat the opposition. The opposition, in turn, tries to regain momentum control by calling time outs to break the cycle of the team on the offense.

OODA Loop Tasks and Attributes

The following tables (tables 1 to 4) list tasks and attributes of each OODA Loop function to demonstrate what should be integrated to enable commanders to control momentum. The objective is to use

the tasks and attributes as measures for how effectively both individual functions and the integrated OODA Loop operates when 2025 technology is applied. Further, the tasks and how attributes serve as measures of merit to determine which technologies discussed in the next chapter meet the requirements to achieve OODA Loop integration. Ultimately, the evolving technologies that rate best seem most appropriate to pursue for system development.

Table 1

Observe Tasks and Attributes

Task	Attributes
See the battlespace	• Fused, integrated, deconflicted view of the desired battlespace • Sum of all possible information sources • System identification of information gaps and subsequent collection of missing information
Maintain mobile battlespace view	• Able to pull updated view anytime, anywhere • Easily deployable and transportable with user
Universal access to battlespace view	• Able to tailor picture for relevant AOR, missions, and tasks • Many able to see the same battlespace picture

Table 2

Orient Tasks and Attributes

Tasks	Attributes
Tailor view of the battlespace	• In-time view of the battlespace • Able to define dimensions and locations of battlespace
Comprehend the battlespace view	• Eliminate biased inputs from one person to another • Eliminate need for mental picture based on another's biases • Able to query for further information; receive in-time answers

Table 3

Decide Tasks and Attributes

Task	Attributes
Decide what is important and what may require action	• Decision support tool in transmitter and receiver to filter, sort, and prioritize • Prompts user of significant events for monitoring and action
Determine action required to rectify undesirable situation	• Model effectiveness of potential actions and inactions with in-time feedback • Optimize application of precision force • Ensure least risk to friendly forces

Table 4

Act Tasks and Attributes

Tasks	Attributes
Immediate access to assets to rectify undesirable situation	• Ready lethal capabilities for employment • Ready nonlethal capabilities for employment • One shot, one kill capability
Feedback on actions and inactions taken	• See in-time mission results • System recommends additional action or inaction

Notes

[1] The concept of a "blue print" has guided US Air Force modernization in the past. Gen Ronald Fogleman, chief of staff, US Air Force, stated in a lecture delivered to the 2025 project participants at Air University, Maxwell AFB, Alabama, 13 February 1996: "Force Modernization is the blue print for [today's tenets of] Global Reach and Global Power. Our strategic vision remains containment through deterrence." To actualize this vision, the Air Force reorganized into Air Mobility Command (Global Reach) and Air Combat Command (Global Power). Further, the 1990s witnessed the Air Force leadership promote the C-17 as the key short-term solution for Global Reach, and the F-22 for Global Power.

[2] Dr Sheila E. Widnall and Gen Ronald R. Fogelman, *Cornerstones of Information Warfare* (Washington, D. C.: 1995), 3.

[3] Fadok, 2.

[4] First Lieutenant Gary A. Vincent, *Operational Structures*, vol. 5, *In the Loop: Superiority in Command and Control* (Maxwell AFB, Ala.: Air University Press, November 1995), 291.

[5] Fukuyama.

[6] Jeffrey McKitrick et al., *The Revolution in Military Affairs*, Air War College Studies in National Security: Battlefield of the Future, no. 3 (Maxwell AFB, Ala.: Air University Press, September 1995), 65–97.

[7] Herbert A. Simon, *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization* (New York: The Free Press, 1976), 38–41.

[8] Lt Col Michael L. McGinnis and Maj George F. Stone III, "Decision Support Technology," *Military Review* 74, no. 11 (November 1994): 68.

[9] Col Richard Szafranski and Col Joseph A. Engelbrecht, Jr., "The Structure of the Revolution: Demystifying the RMA" (Unpublished paper, March 1996), 6–7. The authors used the term *momentum control* to explain time. However, "time is more than speed. It is the attribute of controlled timing or modulating momentum." See also endnote 10, this chapter.

[10] Ralph D. Sawyer, *The Seven Military Classics of Ancient China* (Boulder, Col.: Westview Press, 1993), 442. The concept and description of "momentum control" was derived from the Chinese term, *chieh,* translated as "constraints," which is commonly used to indicate constraints or measures imposed on troops. The term lacks a satisfactory English translation because it encompasses the concepts of "control," "timing," and "measure." See also endnote 9, this chapter.

[11] Ibid.

[12] Szafranski and Engelbrecht, 6–7.

Chapter 3

Technology Investigation

What the warrior needs: a fused real-time, true representation of the warrior's battlespace and the ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute his mission in that battlespace.

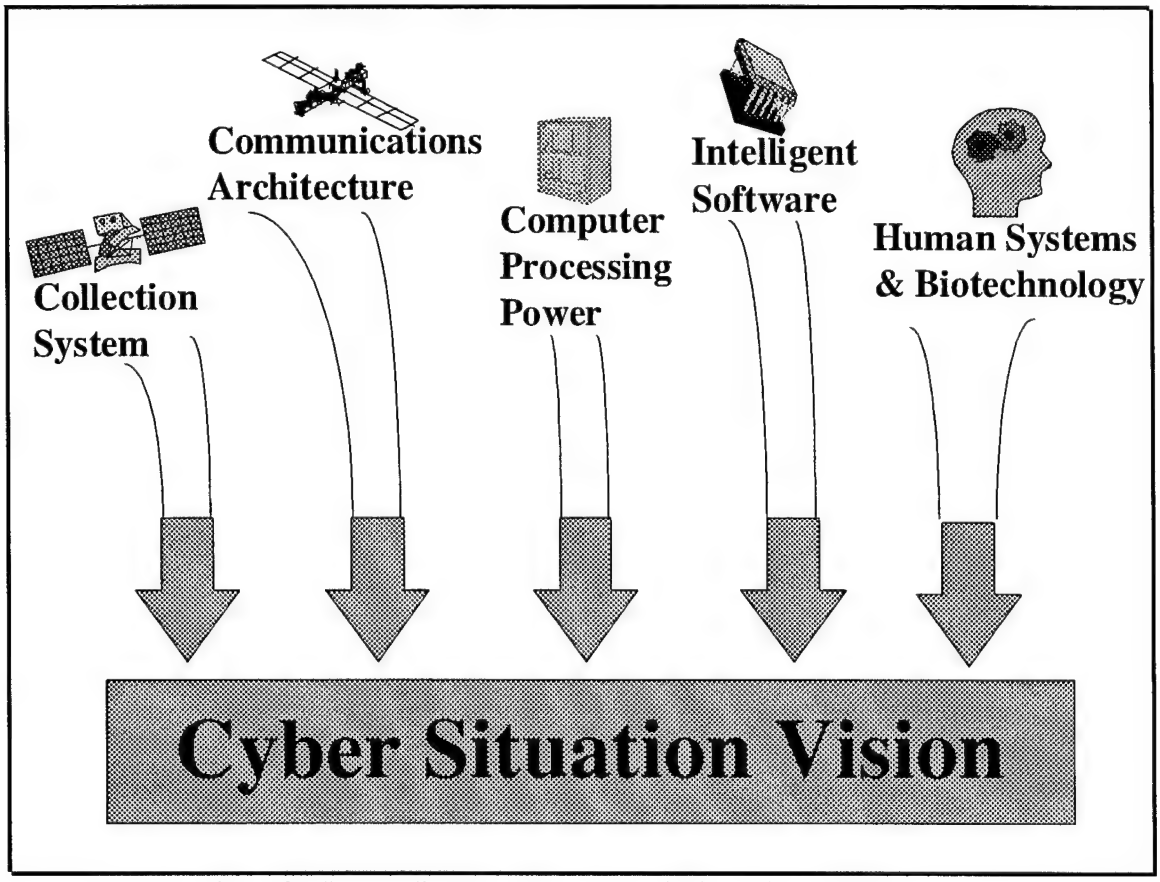
—Adm Richard C. Macke
C4I for the Warrior

In 1992 Adm Richard C. Macke understood what war fighters since Alexander the Great wanted. Information operations is a legitimate and increasingly important military mission that seeks to satisfy Admiral Macke's requirement.[1] Perfecting this capability should allow US military leaders to achieve information dominance and control the momentum of military operations. This vision does not merely provide information, but also empowers users with the ability to leverage information to conduct warfare. This paper refers to this vision as the Cyber Situation. The Cyber Situation is necessary for the US military to maintain its competitive edge against future adversaries.

Technology will provide the means to achieve a complete battlespace picture and the ability to affect it instantly with the Cyber Situation concept. This chapter lays the technological foundation which could achieve this capability. Five broad technology areas should contribute to reaching this goal. Some solutions appear to be evolutionary; some will likely be wildcards—scientifically plausible achievements that will require a technology leap.[2] While this chapter describes the technologies, the next chapter applies these technologies and assesses their contribution to a single system to achieve the Cyber Situation vision.

The Cyber Situation will require five technology areas to evolve and synergize by 2025 to achieve OODA Loop integration. First, collection platforms should provide a detailed global awareness, giving decision makers a complete situational picture.[3] This parallels the observe function of OODA. Second,

communications systems should advance to allow in-time access to virtually any available database. Communications will permit information flow around the loop. Third, computer-processing power and, fourth, intelligent software will provide the ability to integrate and correlate disparate types and sources of information and aid in decision making, contributing to the orient and decide functions. Fifth, human systems and biotechnology advancements will make the man-computer interface seamless. The end result should be an improved ability to access and direct weapons.[4] Figure 3-1 illustrates these essential technologies.



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 3-1. Battlespace Vision Key Components

The following sections address each of these broad technology areas. Within each section, the discussion first relates the particular technology to the required capability in terms of the OODA tasks and attributes (tables 1 through 4). Next, it assesses the current state of the technology and notes which are on evolutionary or revolutionary tracks. It then evaluates various research and development (R&D) trends, focusing on the time and cost needed to achieve the desired technological capability. Most of the

development will be in the commercial arena. Special recognition will be made for those developments that require a military investment.

Collection Platforms

Collection is the process of capturing information from all sources to present an in-time "picture" of the battlespace. In this case, picture refers to more than an image. It is all surveillance and reconnaissance data, including imagery, signals intelligence, weather data, aircraft radar navigation equipment transmissions, cellular telephones and communications devices intercepts, and data in-transit between computers. The list is virtually endless. All information is potentially useful to the Cyber Situation. However, it is not this paper's purpose to exhaustively review all collection technologies. Rather, it will focus on the platforms from which the data and intelligence is received.

Presently, overhead and air-breathing assets collect information. Overhead assets refers to satellite-based systems. They include surveillance, reconnaissance, and target acquisition systems as well as environmental monitoring assets.[5] While many are classified programs, civil and commercial agencies are increasingly able to collect more timely and detailed data. This is particularly true for such environmental monitoring satellites as the French SPOT satellite which can provide multispectral imagery with 10 meter resolution.[6] Air-breathing assets are aircraft, manned or unmanned.

By 2025 collection platforms will exploit the complete electro-optical frequency spectra. Some systems will be deployed for long-durations. These systems will observe such standing requirements as military communications traffic, logistics, and computer interfaces. Some of this capability currently exists. However, the military still lacks sufficiently broad coverage.[7] Other systems may be used on a contingency basis. These systems will use two emerging technologies: miniaturized satellites and uninhibited reconnaissance aerial vehicles (URAV).

Miniature Satellites

The most compelling satellite technologies advances include miniaturization and decreased launch expense.[8] These two complementary advances are important to the system effectiveness of the Cyber

Situation. Increased miniaturization of individual satellites allows for less costly construction per unit and easier deployment while at the same time making them harder to detect and track. Miniature satellite constellations have great applicability in terms of flexibility and deployability.

Miniature satellites could fill coverage gaps to supplement long-duration systems. The miniature satellite constellations would carry payloads optimized for specific contingencies. The payloads may focus on specific static, mobile, or moving targets. This option offers a compelling, inexpensive, and rapidly deployable solution to "customize" collection efforts to meet the contingency needs.[9] The satellites may be constructed en masse and be on hot alert.

While decreased cost for space access is forecasted, miniature satellites are unlikely to garner significant commercial investment. This is not to say miniature components will not be commercially available. Commercial technology initiatives will shrink everything from the solar panels and batteries to the sensors. However, the military must press forward with the R&D to package miniature satellites and make them available for immediate use.

Uninhabited Reconnaissance Aerospace Vehicles

The other emerging technology area for collection platforms is URAV. These systems would provide the data not accessible to either the long-duration assets or the miniature satellite constellations. URAV would reduce the risk inherent in manned collection platforms and allow the flexibility to maneuver rapidly to specific locations which may be obscured from space-based sensors.[10]

The Department of Defense has operated URAV since the Vietnam conflict. Their usefulness will push development of less costly, more reliable, and more flexible systems.[11] One area of flexibility will include more varied sensors that collect all-source information. This area will predominately require military R&D.

The combination of deployed long-duration satellites, small satellites, and URAV could enable the military to achieve broad coverage of an area of interest virtually all of the time, thus providing the user the most updated Cyber Situation possible.

Communication Infrastructure

To achieve information dominance requires high-capacity, secure, accurate, reliable, robust, and easy-to-use communications. Indeed, data and information movement is the track upon which the decision cycle runs. A highly mobile war fighter must be able to maintain an in-time "picture" of the battlespace, formed by vast amounts of information from multiple sources. The user must also be able to communicate with others who are observing the same battlespace picture. Of particular importance is the ability to access and direct weapons at a moment's notice.

Communications must work anywhere and everywhere. Current limitations include narrow bandwidths and insufficient ground-based and satellite infrastructure. In 2025 these limitations will likely be resolved as bandwidth and communications capacities continue to expand.[12]

Although bandwidth is a limiting factor, it has grown dramatically in the last 10 years. The key breakthrough was fiber-optic cabling, which geometrically increased available information flow. Economics drove the development of fiber-optic capability. The marketplace demanded increased throughput, and the private sector responded with a quantum leap over twisted pair (copper wire) technology. Demand will continue to push increased access throughout the country and around the world.[13] Fiber-optic cable will likely be the predominant communication carrier for the foreseeable future, although wireless and satellite communications connectivity also will be required.[14]

Satellite communications are tremendously important because of the need to move large amounts of the information from collection platforms. Current capabilities are inadequate to provide full connectivity and functionality to provide coverage for any given desired place and time. Here, too, technology advances will greatly enhance and improve the ability to move vast amounts of data quickly.

As noted in the previous section, the most compelling satellite technologies advances include miniaturization and decreased launch expense. A significant amount of work has already has been done on the miniaturization of relay and broadcast satellites. To date, experiments have centered on deploying these small satellites over a location where the telecommunications infrastructure is lacking.[15]

On the ground, direct broadcast satellite (DBS) technology use will release commanders and decision makers from the bonds of landlines. It is a fully man-portable satellite receive and transmit ground station.

DBS is commercially available at reasonable cost. DBS groundstations will be able to accommodate large bandwidth and be fully deployable.[16] This is a distinct advantage in terms of flexibility for decision makers at all levels. DBS technology allows on-scene commanders to forward in-time inputs through the system and up the chain of command. Future DBS technology will continue to advance and miniaturize, producing greater capabilities in smaller packages. One challenge is to be able to provide portable power that is not a weight and size burden. Nevertheless, the commercial industry will produce miniaturized, low-power communication devices. As this type of technology improves, DBS might allow human links to satellites. The human body could potentially become a part of the system. "With a little digital help, people's ears could work just as well as 'rabbit ears.'"[17]

Mission accomplishment requires the communications architecture to accurately transmit complete media spectra. More important is the Cyber Situation's need for secure communications. This is a broad category requiring a more detailed discussion.

Security

Since security affects all elements of the OODA Loop, it is best addressed under the communications section. Data must be secured in three different areas: storage, transmission, and dissemination.

Because of the tremendous storage capacity required, archival databases likely will be secured much as they are now, in a vaulted building on shielded media (magnetic, or some evolutionary storage media not yet developed). Storage is discussed in the computer power section below.

The compromise potential is much higher during data transmission, occurs during information collection and routing by way of communications infrastructures. Resident safeguards must protect transmissions from interruption and intercept. Experts expect that this should be easily attained by way of commercially available encryption packages that are nearly unbreakable.[18]

The final security concern involves the process to retrieve, display, and use data. Dissemination security exists to ensure that only those with the appropriate access and need-to-know may use the most sensitive databases. Some promising technologies are already used in this area. Among the most viable are retinal scanners and fingerprint validation technologies developed by the private sector.[19]

Technology could plausibly lead to the use of deoxyribonucleic acid (DNA) samples to validate individual access requirements. The validation system will include each user's DNA imprints, which must be checked before the system allows access. Today, this technology is in its infancy, but, will continue to evolve and likely become the fool-proof way to validate user authenticity for access and employment.

The second type of dissemination security involves technology known as multilevel security (MLS) network management.[20] Upon entering an information system, the system grants access based on the user's authorization. Ideally, MLS allows users with various classification levels to share the same communication architecture and even the same sensors. The difference lies in what each user is able to access in each situation. Since the mid-1980s, the civilian and military communities have conducted R&D in MLS technology. However, the state of technology does not currently allow ideal MLS use. It is reasonable to expect a perfected system by 2025.[21]

Communications Wrap-Up

In large measures, the commercial and military communities already have established necessary communications infrastructure with the National Information Infrastructure (NII) and the Military Information Infrastructure (MII). Both NII and MII are structured to move information in the most expeditious manner, taking advantage of the best of commercial and military communications links. "The MII must able to adapt to unforeseen circumstances, whether induced by the military or by the commercial world. . . It becomes more important to learn to use existing and emerging capabilities in the domain of military applications than it is to develop the capabilities themselves."[22] Thus, the groundwork is already laid for expansion and evolution.

Nevertheless, to fully achieve the 2025 Cyber Situation, a global infrastructure must provide the user a desired view anywhere on earth. Therefore, the 2025 information infrastructure must incorporate both NII and MII—leading to a Global Information Infrastructure (GII).[23]

Effective communications architectures must be robust to accommodate the considerable bandwidth requirements and to harness the full capability of military and civilian communications advances. This leads to the next topic, computer power.

Computer Power

If communications is the track on which the OODA Loop runs, powerful computers is the engines pulling the train. Computers will play a key role in any decision support system to integrate the collected data and present it for orientation and decision making.

Powerful computers with massive storage capacity will be essential in the Cyber Situation. Fortunately, the rapid increases in processing speed and storage, combined with decreased size and energy consumption, will likely continue unabated.[24]

While silicon circuit technology remains viable for the near future, eventually the number of circuits that can be etched will reach a limit.[25] However, researchers are pursuing alternative technologies that should result in even more amazing improvements. They include such exotic concepts as quantum dots and nanomechanical gates.[26]

Biological computing is another promising field which might yield a potential thousandfold computational improvement for one ten-millionth the energy.[27] The concept includes using genetic material from insects to self-assemble into computing elements. House flies and grasshoppers have pattern-recognition abilities which could be applied directly for military and commercial purposes, including cryptography and navigational computation. Initial payoffs to molecular biology computing research may occur in five to 10 years, especially for sensor applications.[28]

Increased speed requires improved data storage media. Again, research shows promise. Holographic memory may allow storage of 64 billion bits on a crystal the size of a compact disk. Activated by a small laser, a single "disk" could contain over 600 hours of music or 30 million pages of double-spaced, typewritten text.[29] Since the data is contained in the laser, it makes it easy to transmit in optical cable as well.[30]

Clearly, by 2025 nearly infinite computations with unlimited storage will be available on tiny machines. It should come with negligible military investment although the *New World Vistas* (NWV) Information Technology Panel warns that defense should continue to fund basic research to keep the "pump primed," else risk less innovation as private research focuses on highly directed problems.[31] However, the challenges of

storage capacity and capability are not the only areas where researchers are trying to stretch the limits. More importantly are increasing the cognitive abilities of the software running on these powerful machines.

Intelligent Software

The most important technology area is the continued advancement of intelligent software. The previous technologies explained how vast quantities of information will be readily available to the war fighter. Without some assistance in managing the load, the commander will suffer from information overload.

Intelligent software is broadly defined as the component programs and algorithms executing on various computer systems. While primarily related to the human's use of the program, it also may operate independently of the user. For example, the collection systems will be able to recognize and identify features, identify information gaps and task a sensor to "fill in the gap," fuse multiple data sources to present an integrated picture, and prompt a user of significant events, all without human assistance. Other software agents will respond to human taskings or augment humans in decision processes.[32] Attributes include the ability to organize and interpret information, simulate and model potential actions, weigh alternatives, and recommend courses of action.

The following paradigm applies for all intelligent systems (biological or computational). This paradigm helps identify and measure the broad intelligent software tools needed for the Cyber Situation.

> All intelligent systems continuously engage in five activities:
>
> . They *perceive* the world.
> . They *interpret* their perceptions in light of their knowledge of the world.
> . They *make plans* based on their current model of the world.
> . They *act* within the world in order to achieve their goals.
> . They *communicate* with other agents to share perceptions and collaborate on execution (emphasis added).[33]

Note the elements of Boyd's OODA Loop in this concept. Many of today's experts envision technological advances will occur in all activities to assist the decision maker. Indeed, the Cyber Situation assumes double-leap improvements in the ability to observe, act, and communicate. The concept focuses on the interpretation and planning activities and how to make the best use of information to plan and execute a military operation.

Intelligent software can be broken down into four broad core technologies:[34]

Image Understanding

Image understanding (IU) seeks to develop mechanisms to create a "description" of the world from sensor images, suitable for particular purposes. The challenge is identification "despite object occlusion, shadows, reflections, and other disturbances."[35] Applying contextual information may be one mechanism to improve the IU process.

IU is a key technology because the Cyber Situation must generate and communicate situational awareness to the user. Within five years, the DOD's Advanced Research Project Agency (ARPA) expects "to carry out applications-directed research on machine vision, provide a suitable IU software environment, and further develop IU capabilities for specific applications." The long-term goal is to "develop computational theories and techniques for use in artificial vision systems whose performance matches or exceeds that of humans, exploiting sensing throughout the breadth of the electromagnetic spectrum, in all environments."[36] Commercial applications include industrial part recognition, visual inspection systems, and indoor robot navigation. However, because of the predominance of military applications, this is a technology requiring DOD investment.

Intelligent Integration of Information

Intelligent integration of information (I3) is the technology to "intelligently process, compile, and abstract useful knowledge from multiple data sources with different interfaces, query languages, data structures, terminology, and semantics."[37] This ability has applications throughout the Cyber Situation. I3 is needed to provide the fused, deconflicted view of the battlespace.

Many valuable applications have been developed. An example is the Air Campaign Planning Tool where planners can now locate high-priority targets in a fraction of the time previously required.[38] However, much work remains to achieve large-scale applications which abstract data from the entire GII. Although commercial applications will push the technology (resulting, for example, in personal assistant

agents sorting increasing amounts of daily electronic mail),[39] the military must invest to obtain the ability to index and then retrieve images based on military semantics.[40]

Planning and Decision Aids

Planning and decision aids (PDA) tools develop representation and reasoning techniques to generate and analyze plans and schedules. These tools are necessary to help the user (or users) make correct and timely decisions, thus deconflicting information overload. The tools will "reduce problem solving time by orders of magnitude while at the same time increasing the number of options considered by orders of magnitude."[41]

The concept of PDAs is well understood, as it is simply an implementation of such decision theories as linear programming and quantitative analysis. What is new is the ability to employ these techniques on a high-speed computer. Many techniques already exist, both in private and military use. One example is the Dynamic Analysis and Replanning Tool which was used in Desert Storm.[42] Commercial applications, both executive and group support systems, also are being adapted for military use. The military must focus on ensuring more than one user can use them simultaneously and that the tools capture the planning rationale.[43]

Human Computer Interaction

Human computer interaction (HCI) will "develop techniques and environments to provide informative, intuitive, and taskable access and control over complex software."[44] This environment is another key area for the Cyber Situation--being able to "interact in a natural fashion with speech, gesture, and other advanced interaction techniques." Eventually, it should include brain activated control. A goal is for many users able to interact over computer networks.

Initially, human language system advances will be where the most significant work is done. However, the NWV Information Technology Panel suggest handwriting recognition will become prevalent as well as speech recognition capabilities within 10 years. While the currently dominant keyboard-display-mouse configuration will remain, newer generations of users will become more comfortable with more natural interfaces. By 2025 technology will have matured such that handheld, portable "personal assistants" will be

available. Additionally, virtual and augmented reality systems and telepresence models also will be in use. Telepresence models allow a human access to otherwise inaccessible locations. Applications include microsurgery, space system repair, and microelectronic machine assembly.[45]

The NWV Human Systems and Biotechnology Panel describes neuroscience as a promising research area. As science improves our understanding of the brain and how it functions, it makes it possible to direct equipment to respond to our thoughts, without any verbal or written command. Already, preliminary research using an 128-sensor array electroencephalograph (EEG) pressed against a subject's skull can "influence information content and display designs on a computer screen.[46] This concept is discussed further in the next section. Commercial and medical organizations will take the lead in developing this technology. Neuroscience developments will continue.

Human Systems and Biotechnology

The human-computer systems integration is a vital lead-in to the final technology area. Human systems and biotechnology offers the potential to create a seamless flow of information between human and computer. By exploiting the human cognitive process, it can be tailor information to present precisely what is needed.

This section is divided into two parts. The first is understanding information flowing to and from the brain. The second is how to present that data using visual-imaging techniques. Mastering these technologies will allow users to select information for direct input into their brains. However, regardless of how advanced a decision system becomes, a human will be in the loop. The best technology can only help, but in the end, the person, not the machine, ultimately makes the decision.

Charting the Brain

Thirty years ago little was known about the brain. Great advances have been made in the last 10 years, and much has been learned about information flow out of the brain and the way it interacts with the neural network.[47] Understanding how information enters the brain and how it is processed will form the foundation for the ultimate in human-computer interface. "Success in transducing and translating brain waves allows

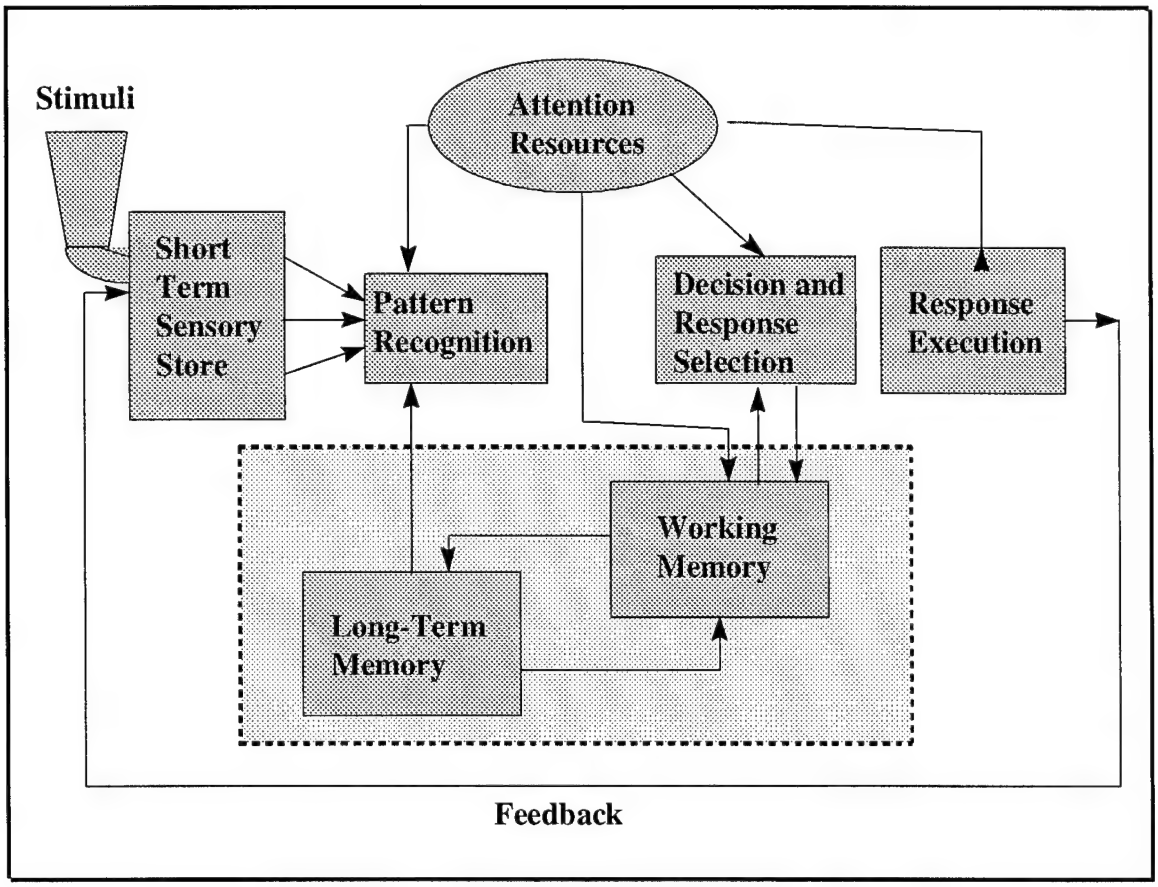
people to interface with specific systems, perhaps sensed through transducers in a headband or another such brain-machine connection."[48]

Two research areas are critical to the human computer interface. The first of these is, charting and understanding information flow out of the brain. The second, and more applicable, is information flow into the brain. Understanding of human systems such will enable more rapid processing of data and more efficient use of the provided information.

Charting information out of the brain is a complex effort. However, much work has been done in this area.[49] Mechanical methods have been fielded to emulate, and in some case replicate, these complex processes.[50] Intelligent materials, including fiber-optics and piezioelectric materials, are two techniques under development to try to replace damaged or destroyed neuron-actuation sensor networks in humans.[51]

In principle, data flowing out of the brain is in the form of electronic impulses which actuate the neurostructure within humans.[52] Recent research has charted the source of some basic impulses within the brain, identified precisely what neuron network is actuated by electric impulses, and determined what action is completed by the network.[53]

Charting information flow *into* the brain and how the brain processes it once inside is even more difficult. This effort requires understanding how the brain formats the data to make decisions. Each human's information process is unique, based on such factors as experiences, learning, intelligence, and personal biases.[54] Science is attempting to understand the commonalities between humans.[55] Some work has been done to chart the essentials of human information processing fig. 3-2.[56]



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 3-2. Human Information Processing Flow[57]

Computers can play a significant role in nearly every area of human-information processing. Their potential lies in organizing information to assist human decision making. They can produce more options than a human brain can recall.[58] In fact, computers have become the preferred medium for information storage and recall.[59]

However, a gap still exists in the information flow between humans and computers. Information is processed by a human looking at a screen, reading the data, and translating it into something useful through internal thought. "We talk longingly about human-computer interactions and conversational systems, and yet we are fully prepared to leave one participant in this dialogue totally in the dark. It is time to make computers see and hear."[60] Users should "converse" with computers. Intelligent systems outlined above provide only part of the answer to improve human-computer interaction. The missing piece is a better way to

format and transmit information from the digital computer processor in the computer chip to the analog human processor in the human brain.

Instead of formatting a cathode ray tube (CRT) to more easily access and display data, a computer can be designed and programmed to bypass the CRT and format information which can be immediately processed by the brain. The logical extension would be to place the human computer interface directly in the brain. Some significant progress already has been made in this area by the Stanford University research center and their development of a nerve chip.

> It is an electronic interface for individual nerve cells to communicate with a computer. This human-machine linkage will. . . enhance human capability in many ways. If artificial eyes can convert video to nerve signals, won't it be possible to use the same technique to superimpose computer-generated information in front of one's field of view?[61]

This capability will have extraordinary commercial applications from medical advances. These advances will help restore patients with damaged neural, audio, and visual systems as well as enable individuals to achieve the "ultimate virtual reality trip."[62]

Visualization and Mental Imaging

This second broad category encompasses a realm of the cyberspace essential to the concept. Developing technologies are based around the idea of virtual projection systems that evolve into holographic image projection. The National Center for Supercomputing Applications Virtual Reality Laboratory "is a research facility engaged in the exploration of new methods of visualizing an interfacing with scientific data and simulations."[63] To further their objectives, they have created the CAVE a "surround-screen surround-sound, projection-based virtual reality system." [64] Multiple participants can enter the CAVE and interact by wearing stereo glasses rather than a helmet. "The CAVE can be coupled to remote data sources, super computers and scientific instruments via high-speed networks."[65] The NWV Information Technology Panel considers significant virtual reality advancements in the next 10 to 20 years. However, the display mechanism will primarily involve a helmet.

Commercial applications are easy to envision, witness the growing entertainment market for virtual reality games. This appears to be the next step from video teleconferencing. Another useful application will

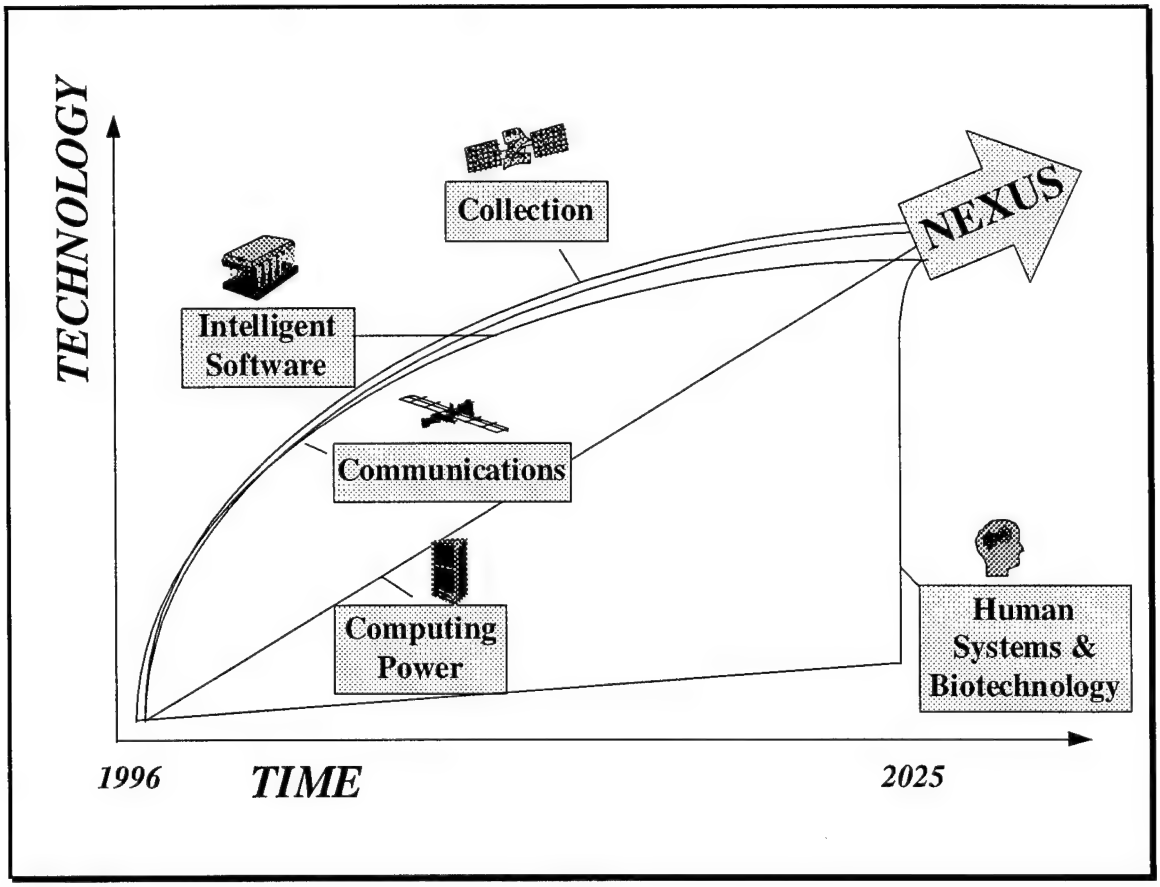
be for training systems—especially simulations.[66] This has wide commercial applications, especially as future systems will require such high-knowledge levels to use them as transportation and manufacturing.

A more specific military application of this type of technology is the DOD simulation network (SimNet). This capability allows a simulator to emulate a battlefield precisely. Trainees sit in their own aircraft or tank simulator and are able to "view" the battlefield from their own perspective. "Army tankers in trainers in Fort Knox can look out of their sites and see the same location—only from each of their individual perspectives. Air Force pilots in California can 'fly' missions . . . at the same time."[67]

A combination of brain processes and visual imaging already has been developed in the laboratory. The California Institute of Technology has developed an energy efficient computer chip which emulates the analog thinking of the human brain. It is specifically modeled on the construction of the human brain, specifically the cerebral cortex.[68] When this capability is fully mature, this chip could provide the baseline for a brain implant hooked to the all the sensory segments of the brain, not just the eye.

Bringing It Altogether--The Nexus

While each technology area will progress at a unique rate, the challenge is to bring them together to reach their synergistic peak--the nexus (fig. 3-3).



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 3-3. Development Lines for System Elements

Collection. Collection capability will be complete when there is no want of information. The various constellations of permanent satellites complimented by the mini satellites will provide coverage of the entire world in every spectrum. Collection development should continue to grow until about 2015, when the complete link between the small satellites and the permanent constellations should be seamless, and the small satellite development will be commensurate with the requirements.[69]

Communications. Communications capacity will peak when the entire globe is accessible at all times and there is absolutely no restriction on the size or type of transmission available to the customer. The web of commercial, government, and military networks will be seamless, and only the speed of light will delay information movement. There is much effort underway, both in the commercial and military sector, to achieve this connectivity. Development of new systems and new capabilities should reach this goal by 2010.[70]

Computing power. Computing power will continue to grow in capacity, doubling every 18 months for the near term.[71] As noted, analysts have frequently thought the silicon chip had reached its maximum capacity, then discovered through increased micronization that more capacity could be obtained. However, most analysts believe that the silicon chip will hit its peak between 2015 and 2020.[72] If true, R&D efforts will continue to search for other media to store and process data.

Intelligent Software. Intelligent software is increasing in its availability but has yet to fully meet the requirements of the Cyber Situation. More effort is required to allow full capability of intelligent systems and bring that technology to bear on an advanced decision tool. Current intelligent software development is not well articulated, and the specific capability of the software is left to systems designers and engineers meeting the demands of a specific program.[73] Thus, much of the development of intelligent systems is linear and relates only to the requirements of a specific program. Such a design is not conducive to interaction and broader application.

Human Systems and Biotechnology. This area requires the most work to achieve the Cyber Situation. Work is expected to continue at a modest pace until a breakthrough in the this technology is achieved.[74] Like many advanced research areas, work here will require one big leap over a single chasm. In this case, the chasm is understanding the way information is formatted in the brain and how it is used. Once this chasm is achieved, progress in human computer interaction will grow exponentially and quickly catch up with the other technology areas.

By 2025 the five technology areas will be effectively linked to develop the Cyber Situation to enable commanders to achieve information dominance. The next chapter will describe the Cyber Situation system, its components, and how it meets the attributes of the OODA Loop tasks.

Notes

[1] Widnall and Fogleman, *Cornerstones on Information Warfare,* 11.

[2] John L. Peterson, *The Road to 2015: Profiles of the Future* (Corte Madera, Calif.: Waite Group Press, 1994), 288. Peterson states, "Wild cards have a low probability of occurrence but a very high impact."

[3] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century* (unpublished draft, the information applications volume, 15 December 1995), 68.

[4] *New World Vistas,* (unpublished draft, the human systems and biotechnology volume), 8.

[5] Army Space Institute, *Theater Air Campaign Studies*, vol. 8, *Space Support in Mid-Intensity Conflict* (Maxwell AFB, Ala.: Air University Press, 1995), 306–9.

[6] Ibid., 308.

[7] *New World Vistas,* (unpublished draft, the information technology volume), 85.

[8] Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1995), 35–36.

[9] Lt Col Henry Baird et al., "Spacelift" (Unpublished 2025 research paper, Air University, Maxwell AFB, Ala., April 1996); 2025 Concept, No. 900552, "On-demand Tactical Recce Satellite Constellation," 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996).

[10] Numerous 2025 Concepts dealt with this technology to include:

2025 Concept, No. 900272, "Very High Altitude Balloon-Borne Systems," 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996); 2025 Concept, No. 900280, "Fly on the Wall," No. 900434, "Airborne Sound Sensors," 2025 Concepts Database,(Maxwell AFB, Ala.: Air War College/2025, 1996); 2025 Concept, No. 900438, "Ultraendurance High-Altitude Ocean Loitering Uninhabited Reconnaissance Vehicle," 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996); 2025 Concept, No. 900517, "JSTARS Replacement," 2025 Concepts Database,(Maxwell AFB, Ala.: Air War College/2025, 1996); and 2025 Concept, No. 900604, "UAV Constellations," 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996).

[11] Lt Col Bruce Carmichael et al., "StrikeStar 2025" (Unpublished 2025 research paper, Air University, Maxwell AFB, Ala., April 1996), 94-95. Particularly, the appendix describes the historical reliability problems with UAV.

[12] Alvin and Heidi Toffler, *War and Anti War* (New York: Warner Books, 1993), 90–91.

[13] Negroponte, 21–36.

[14] *New World Vistas,* (unpublished draft, the information applications volume), 32–46.

[15] A senior US Air Force policymaker lecture given to the 2025 Study Group under the promise of nonattribution

[16] Aleksandar Kolarov and Joseph Hui, "Least Cost Routing in Multiple-Service Networks: Part II," On-line, Internet, September 1995, available from http://www.research.att.com/hgs/infocom95/program.html.

[17] Negroponte, 211.

[18] *New World Vistas,* (unpublished draft, the information technology volume), C-3.

[19] There are several different authentication technologies. The retinal (eye) scanner is currently used at Falcon AFB, Colorado.

[20] Makoto Takano and Katsumi Fujita, "Multilevel Network Management by Means of System Identification," On-line, Internet, September 1995 available from http://www.research.att.com/hgs/infocom95/program.html.

[21] Charles Kalmanek and K.G. Ramakrighnan, Third International Telecommunications Symposium, "On-line Routing for Virtual Private Networks," On-line, Internet, September1995, available from http://www.research.att.com/hgs/infocom95/program.html; Lt Col James McMillan, Air Force Liaison to National Security Agency, telephone interview by Maj Scott Bethel, 26 February 1996. MLS has been a long-standing DOD problem both in the US only (collateral versus SCI) and in releasing data to foreign nationals. The main problem is with data at different classification levels using the same communication architecture: how to prevent inadvertent or targeted database access at a higher classification level through lower channels.

[22] *New World Vistas,* (unpublished draft, the information applications volume), 52.

[23] Institute for National Strategic Studies, *Strategic Assessment 1995: US Security Challenges in Transition* (Washington, D. C.: National Defense University Press, November 1994), 151.

[24] *New World Vistas,* (unpublished draft, the information technology volume), 1, 87–90.
Peterson, 28–30.
David A. Patterson, "Microprocessors in 2020," *Scientific American* 273, no. 3 (September 1995): 48–51.

[25] *New World Vistas,* (unpublished draft, the information technology volume), 87.

[26] Patterson, 51.

[27] Clarence A. Robinson, "Molecular Biology Computation Captures International Research," *Signal* 50, no. 6 (February 1996): 17–21; Thomas A. Bass, "Gene Genie," *Wired* (August 95): 114–17, 164–68.

[28] Robinson, 21.

[29] Demetri Psaltis and Fai Mok, "Holographic Memories," *Scientific American* 273, no. 5 (November 1995): 70-76.

[30] *New World Vistas,* (unpublished draft, the information technology volume), 24. This document suggests "the communications laser will replace the microprocessor as the key enabling technology shaping the personal computer industry."

[31] Ibid., 29. The document also suggests battery performance may be a limiting factor.

[32] Advanced Research Program Agency, "The SISTO Solution: Intelligent Software Systems," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Solution.hmtl. SISTO is the Software and Intelligent Systems Office of the Advanced Research Program Agency.

[33] Ibid.

[34] Advanced Research Program Agency, "Intelligent Systems," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Intel_Thrust.html.

[35] Oscar Firschein and Thomas Strat, "Image Understanding Program," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Image.html.

[36] Ibid.

[37] David Gunning, "Intelligent Integration of Information (I3)," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/I3.html.

[38] Ibid.

[39] *New World Vistas,* (unpublished draft, the information technology volume), 38-44.

[40] Ibid., 13.

[41] Dr Tom Garvey, "Planning and Decision Aids Program," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/PDA.html.

[42] Ibid.

[43] *New World Vistas,* (unpublished draft, the information technology volume), 13.

[44] Allen Sears and Robert Neches, "Human Computer Interaction Program," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/HCI.html.

[45] *New World Vistas,* (unpublished draft, the information technology volume), 37.

[46] Ibid., 24.

[47] Peter Thomas, "Thought Control," *New Scientist* 149, no 2020 (9 March 1996): 39. The University of Utah has done significant work to map the brain. Through a series of some 100 sensors implanted in the brain, this team effectively mapped the parts of the brain that see and hear. Their focus was to reformat information to restore sight to the blind. They reported limited success as some of their research subjects claim to "see" words in their mind while reading them in Braille.

[48] Peterson, 293.

[49] Henry Petroski, *To Engineer is Human* (Chicago: University of Chicago Press, 1989), 216.

[50] Craig A. Rogers, "Intelligent Materials," *Scientific American* 273, no. 3 (September 1995): 123.

[51] Ibid., 124.

[52] Thomas, 38-42.

[53] Ivan Amato, "Animating the Material World," *Science* 225 (17 January 1996): 284–286.

[54] Thomas, 40.

[55] Petroski, 211.

[56] Thomas, 39; *New World Vistas,* (unpublished draft, the human systems and biotechnology volume), F-1.

[57] *New World Vistas,* (unpublished draft, the human systems and biotechnology volume), F-2.

[58] Thomas., 40.

[59] Ibid., 41.

[60] Negroponte, 128.

[61] Peterson, 63.

[62] Ibid., 41.

[63] Bill Sherman, "NCSA Virtual Reality Lab & CAVE," On-line, Internet, 18 February 1996, available from http://www.ncsa.uiuc.edu/VR/VR.html. The laboratory is located at the University of Illinois at Urbana-Champaign.

[64] NCSA VRL, Electronic Visualization Lab, University of Illinois at Chicago, "The CAVE: A Virtual Reality Theater," On-line, Internet, 18 February1996, available from http://www.ncsa.uiuc.edu/EVL/docs/html/CAVE.html.

[65] Ibid.

[66] *New World Vistas,* (unpublished draft, the information technology volume), C-6–C-7.

[67] Peterson, 46.

[68] Ibid. 32.

[69] A senior US Air Force policymaker lecture given to the 2025 Study under the promise of nonattribution.

[70] George I. Zysman, "Wireless Networks," *Scientific American* 273, no. 3 (September 1995): 51.

[71] Negroponte, 64.
Rogers, 122.

[72] Negroponte, 64.
Rogers, 124.

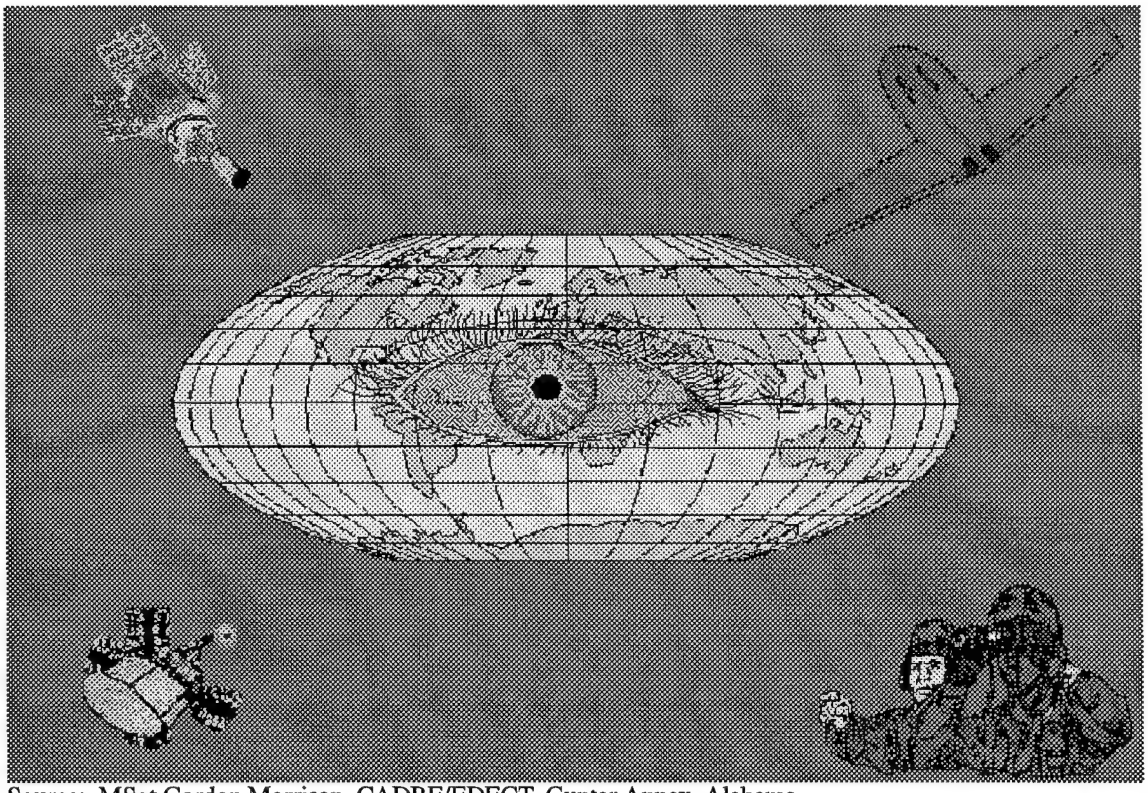
[73] *New World Vistas,* (unpublished draft, the information technology volume), 38.

[74] Thomas, 41.

Chapter 4

System Description

The vast array of technologies, concepts, and innovations in the previous chapter described the pieces that must be integrated to form the "Cyber Situation Vision." As seen in fig 4.1, the Cyber Situation Vision provides a commander with an "eye to see" all within a given battlespace.

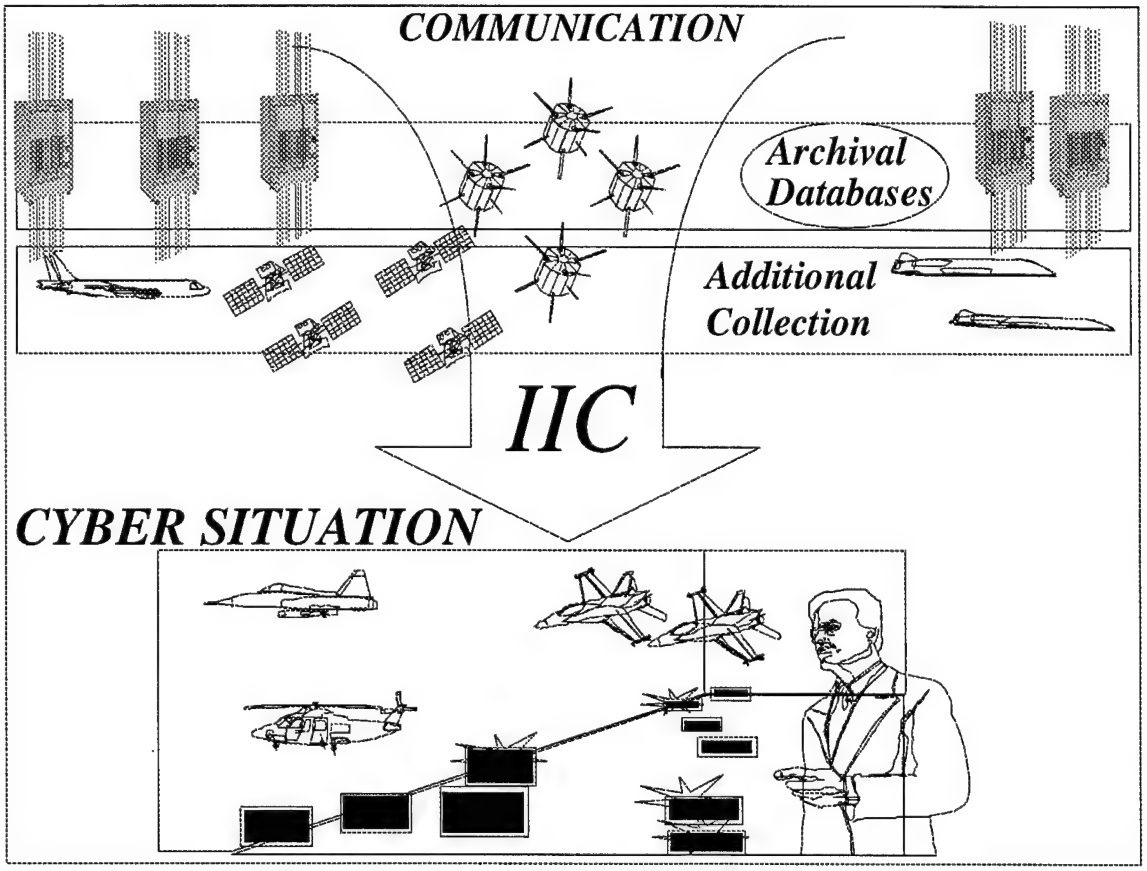


Source: MSgt Gordon Morrison, CADRE/EDECT, Gunter Annex, Alabama

Figure 4-1. Cyber Situation Vision: "Eye" See Everything[1]

Cyber Situation Components

The Cyber Situation is the integration of the entire OODA Loop Cycle under the control of commanders, decision makers, and analysts. Supporting components include all-source information collectors, archival databases, the Information Integration Center (IIC), a microscopic chip implanted in the user's brain,[2] and a wide range of lethal and nonlethal weapons.



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 4-2. Cyber Situation Components

This chapter first describes the five Cyber Situation system components which could result from technological advances. Next, it relates these advances to each system component (table 5). It then describes Cyber Situation integration and focuses on developing the two key components to achieve information dominance and seamless interface between the users and systems—the IIC and microscopic chip (the third and forth components). The first two components (information collectors and databases) provide the inputs, while the fifth component (lethal and nonlethal weapons) is the link to the act—the end product that results

from a system that provides battlespace awareness. Finally, this chapter compares and evaluates the system capabilities with the requirements discussed in chapter 2.

Table 5

Technology Areas Versus Cyber Situation Components

	Technology Areas				
Cyber Situation Component	Collection Platform	Communications Infrastructure	Computing Power	Intelligent Software	Human Systems & Biotechnology
All-source Information Collectors	X	X	X	X	
Archival Databases	X	X			
IIC		X	X	X	X
Implanted Microscopic Chip		X	X	X	X
Lethal & Nonlethal Weapons		X	X		

All-Source Information Collectors

All-source information collectors will transmit raw data to the IIC, discussed below. The collectors are linked by way of high-speed relay and dissemination systems. The collection platforms, in air and space, will be numerous and flexible.

Archival Databases

Archival databases will be used for historical analysis and to fill gaps if the information is not available for collection. Much of the archival data will be resident in the GII, while secured permanent ground stations will store classified data.

IIC

The IIC is a constellation of integration or "smart" satellites that receives all-source information. Within the IIC, resident intelligent software will run decision support tools, correlate and fuse data into

useful information, identify inconsistencies and information gaps, and task collectors to seek data to fill information gaps.

Implanted Microscopic Chip

The implanted microscopic brain chip[3] performs two functions. First, it links the individual to the IIC, creating a seamless interface between the user and the information resources (in-time collection data and archival databases). In essence, the chip relays the processed information from the IIC to the user. Second, the chip creates a computer-generated mental visualization based upon the user's request. The visualization encompasses the individual and allows the user to place himself into the selected battlespace.

Why the Implanted Microscopic Chip? While other methods such as specially configured rooms, special helmets, or sunglasses may be used to interface the user with the IIC, the microscopic chip is the most viable. Two real operational concerns support the use of implanted chips and argue against larger "physical" entities to access the Cyber Situation.

First, future operations will demand a highly flexible and mobile force that is ready at moment's notice to employ aerospace power. The chip will give these forces the ability to communicate, visualize, and prosecute military operations. Having to manage and deploy a "physical" platform or room hampers mobility and delays time-sensitive operations. US aerospace forces must be prepared to fight or to conduct mobility or special operations anywhere in the world on extremely short notice although some of these operations may be staged directly from the continental United States.[4]

Second, a physical entity creates a target vulnerable to enemy attack or sabotage. A highly mobile information operations center created with the chip-IIC interface makes it much more elusive to enemy attack. These reasons argue against a larger physical entity for the Cyber Situation.

While this is a reasonable portability rationale for the use of chip, some may wonder, "Why not use special sunglasses or helmets?" The answer is simple. An implanted microscopic chip does not require security measures to verify whether the right person is connected to the IIC, whereas a room, helmet, or sunglasses requires additional time-consuming access control mechanisms to verify an individual's identity and level of control within the Cyber Situation.

Further, survey any group of commanders, decision makers, or other military personnel if they enjoy carrying a beeper or "brick" at all times. Likely, few like to carry a piece of equipment. Now, imagine having to maintain a critical instrument that allows an individual to access the Cyber Situation, and thus control the US military forces. Clearly, this is not an enviable position, since the individual may misplace or lose the helmet or sunglasses, or worse yet, the enemy may steal or destroy it. These are unnecessary burdens.

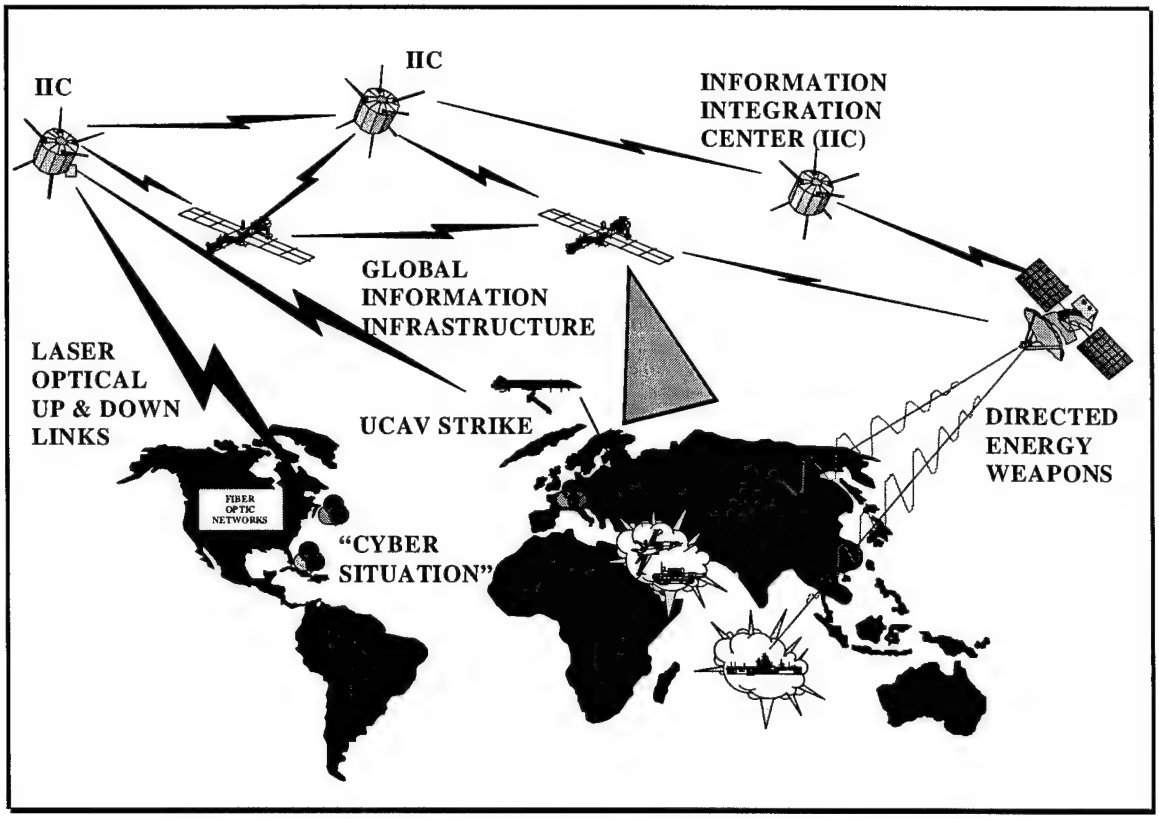
Ethical and Public Relations Issues. Implanting "things" in people raises ethical and public relations issues.[5] While these concerns may be founded on today's thinking, in 2025 they may not be as alarming. We already are evolving toward technology implanting. For example, the military currently requires its members to receive mandatory injections of biological organisms (i.e., the flu shot). In the civilian world, people receive mechanical hearts and other organs. Society has come to accept most of these implants as a fact of life. By 2025 it is possible medical technology will have nerve chips that allow amputees to control artificial limbs or eye chips that allow the blind to see.[6] The civilian populace will likely accept an implanted microscopic chips that allow military members to defend vital national interests. Further, the US military will continue to be a volunteer force that will freely accept the chip because it is a tool to control technology and not as a tool to control the human.

Lethal and Nonlethal Weapons

A wide range of lethal and nonlethal weapons will be linked to the IIC, allowing authorized users to directly employ these weapons. A user's authority to employ weapons will depend on the person's position, responsibility, and rank.

Putting It Together

The Cyber Situation is not a traditional operations or command and control center. Not a physical infrastructure, it consists of many components geographically dispersed, redundant, and networked. When an authorized individual needs situational updates and analyses, the user will link to an IIC satellite by way of the implanted chip.



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 4-3. Cyber Situation Connectivity

The Cyber Situation is applicable at all levels of war. At the strategic and operational levels, it provides the user the capability to monitor global activity, analyze developing situations, monitor and control the battlespace, assess battle damage, and conduct reconstitutions. Tactically, the Cyber Situation offers battlespace situational awareness by conveying in-time enemy and friendly information. At all levels, the Cyber Situation gives decision makers and analysts the ability to coordinate, respond, and execute battlespace operations.

Measures of Merit

Thus far, this paper has shown how the five key technology areas (collection platforms, communications architecture and dissemination systems, computer-processing power, intelligent software, and human systems and biotechnology) will logically synergize by 2025 to realize the Cyber Situation vision to enable information dominance. The paper asserts that to achieve this vision, technology must allow military

commanders to integrate the functions of the OODA Loop and enable the military commander to control momentum. Whether Cyber Situation meets the goal is best answered by evaluating the Cyber Situation against the measures of merit developed in chapter 2. The measures of merit encompasses a list OODA Loop tasks with associated attributes that describes how the task should be performed.

Observe Tasks

Table 6

See the Battlespace

Attributes	Yes or No
• Fused, integrated, and deconflicted view of the desired battlespace	Yes
• Sum of all possible information sources	Yes
• System identification of information gaps and subsequent collection of missing information	Yes

The IIC component of the Cyber Situation provides the avenue to meet the attributes of this "see the battlespace" task. The IIC includes an inherent capability to fuse, correlate, and deconflict available all-source information. Further, built into the system description is the ability to identify information gaps. Links allow the IIC to task collection assets to fill information gaps and deconflict contradictory information. If the collection assets are not able to obtain further information, the IIC uses historical archival databases to fill in gaps. Accordingly, the IIC lets the user know the picture's reliability.

Table 7

Maintain Mobile Battlespace View

Attributes	Yes or No
• Able to pull updated view anytime, anywhere	Yes
• Easily deployable and transportable with user	Yes

Within the Cyber Situation vision, the ability to maintain a "mobile" battlespace picture is perhaps its most significant characteristic. The use of the implanted microscopic chip linked to the IIC allows the user to pull a computer-generated mental visualization of the desired battlespace anytime, anywhere. Further, the

user is not confined to any physical room or platform to enter the Cyber Situation system, making it impenetrable. Even more advantageous, the user has no worry of losing or having someone steal the microchip because it is not a detached physical entity that requires accounting and protection.

Table 8

Universal Access to Battlespace View

Attributes	Yes or No
• Able to tailor picture for relevant AOR, missions, and tasks	Yes
• Many able to see the same battlespace picture	Yes

The IIC allows virtually unlimited number of users to simultaneously access the system because it operates on the user-pull concept. This system's characteristic allows multiple users to access the same battlespace picture and create a "cyber conference" within the Cyber Situation system. Further, IIC's resident intelligent software, coupled with taskings transmitted by way of the chip, allows the user to define the battlespace picture dimensions. This process enables the user to tailor the battlespace computer-generated mental visualization to the relevant area of responsibility (AOR), mission, and tasking to prosecute military operations.

Orient Tasks

Table 9

Tailor View of the Battlespace

Attributes	Yes or No
• In-time view of the battlespace	Yes
• Able to define dimensions and locations of battlespace	Yes

Since the IIC uses the most current data to create battlespace picture, the user's mental visualization will be the most up-to-date information available. As with the previous task, IIC resident intelligent software, coupled with taskings transmitted by way of the microscopic chip, allows the user to define the battlespace picture dimensions.

Table 10

Comprehend the Battlespace View

Attributes	Yes or No
• Eliminate biased inputs from one person to another	Yes
• Eliminate need for mental picture based on another's biases	Yes
• Able to query for further information and receive in-time answers	Yes

Commanders using the Cyber Situation system receive battlespace information that is less biased than the same information when conducted by human processing, interpretation, and presentation. Further, the system minimizes the need for the commanders to mentally reconstruct the information presented by analysts and briefers. If the users sense the battlespace picture does not logically compute, or if they just want additional information, they may request the IIC confirm the situation. The IIC then tasks additional collection assets to seek further data and searches the archival database for further analysis.

Decide Tasks

The IIC acts both as a receiver and as a transmitter. As a receiver, it accepts data from collection assets, users' queries for additional information, and commander's orders to employ remote weapons, space-based lasers, and UCAV. As a transmitter, it responds to users' information requests, prompts users of significant events, tasks collection assets, and relays orders from the users to space based lasers and UCAV to employ weapons. Within the transmitter and receiver components of the IIC, intelligent software automatically filters, sorts, and prioritizes data for processing and fusing. Ultimately, the IIC prompts the user of significant event and the user decides whether action is required for the situation.

Table 11

Decide What is Important and What May Require Action

Attributes	Yes or No
• Decision support tool in transmitter and receiver to filter, sort, and prioritize	Yes
• Prompts user of significant events for monitoring and action	Yes

As a decision aid, the Cyber Situation system allows users to model outcomes of potential actions and inactions to determine the optimum course of action. The modeling process lets the user best apply precision force at the least risk to friendly forces to achieve military objectives.

Table 12

Determine Action Required to Rectify Undesirable Situation

Attributes	Yes or No
• Model effectiveness of potential actions and inactions with in-time feedback	Yes
• Optimize application of precision force	Yes
• Ensure least risk to friendly forces	Yes

Act Tasks

The IIC will be linked to such lethal and nonlethal assets as space-based laser and various UAV. The authorized user will have immediate access to these assets to rectify an undesirable situation. Precision-force assets could allow users to optimize weapons to achieve one shot and one kill.

Table 13

Immediate Access to Assets to Rectify Undesirable Situation

Attributes	Yes or No
• Ready lethal capabilities for employment	Yes
• Ready nonlethal capabilities for employment	Yes
• One shot, one kill capability	Yes

Upon taskings from authorized users to employ space-based laser assets and UAV, the IIC also will task collection assets to accumulate data from the target. The IIC then processes and analyzes the data to provide in-time feedback to the users. It also recommends additional actions if the target is not satisfactorily affected.

The Cyber Situation system could change dramatically how commanders process information and take action or cycle information through the OODA Loop. To be effective, the Cyber Situation system be optimized to minimize vulnerabilities. The next chapter reviews those potential weaknesses and countermeasures.

Table 14

Feedback on Actions and Inactions Taken

Attributes	Yes or No
• See in-time mission results	Yes
• System recommends additional action or inaction	Yes

[1] Special thanks to MSgt Gordon Morrison, CADRE/EDECT, The Extension Course Institute, Air University, Gunter Annex, Maxwell AFB, Ala., for his depiction and creation of the "Cyber Situation," 25 March 1996.

[2] 2025 Concept, No. 900702, "Implanted Tactical Information Display," 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996).

[3] 2025 Concept, No. 200169, 2025 Concepts Database (Maxwell AFB, Ala.: Air War College/2025, 1996).

[4] Peter Grier, "New World Vistas," *Air Force Magazine*, March 1996, 20.

[5] Anonymous assessor comment on 2025 Concept Identification 900702, 2025 Concept Database (Maxwell AFB, Ala.: Air War College/2025, 1996).

[6] John L. Peterson, *The Road to 2015*, Waite Group Press (Corte Madera, Calif. 1994), 63.

[7] Col Joseph A. Engelbrecht, Jr., 2025 research director, and professor of Conflict and Change, Air War College, Maxwell AFB, Ala., personal interview with Major Whitehead, 17 March 1996. Colonel Engelbrecht explains that "Eliminating human biases may be impossible. Since the decision is reserved for the commander or decision maker, the potential for bias may always remain. On the other hand, communication theory and prospect theory from psychology suggest the importance of how the message is "framed." Framing the message can set up a bias in the human receiver. Thus, potentially, technology should be able to help by providing alternate frames or contexts or highlighting a perspective highly relevant for the data and circumstance. While designing the technology to meet the challenge may be difficult, if it is not pursued humans may be trapped in a noisy cacophony of inputs that become screened or skewed simply because little progress has been made in human-machine interfaces."

Chapter 5

Vulnerabilities and Countermeasures

Identifying vulnerabilities of the Cyber Situation and its associated components, then developing potential countermeasures, leads to additional features and attributes that should be integrated into the Cyber Situation requirement list. This chapter begins by identifying vulnerabilities of the Cyber Situation and then states possible countermeasures that eliminate the vulnerabilities.

Vulnerabilities

Numerous vulnerabilities of the Cyber Situation system and its associated components exist. The vulnerabilities naturally fall into three primary categories man-made threats (space debris and offensive weapons), environmental threats (meteors, asteroids, and radiation), and human threats (capture, defection, and espionage).

The first threat area, man-made, generally designed to destroy, disable, or degrade its targets. The effects may be either permanent or temporary and may consist of hard and soft attacks. Adversaries achieve "hard kills" by physical destruction of the Cyber Situation through destruction of system components. Specific methods of attack may include antisatellite weapons, electromagetic pulse (EMP) weapons, and nuclear detonation devices. Conversely, "soft kills" attack the internal logic within the operating capability. An example of soft attack is syntactic attacks of the operating logic inside the IIC and collection computers. The resultant loss or decrease in effectiveness, if not replaced in a timely manner, will have dire consequences on military operations.

Less obvious military vulnerabilities come from the second threat area, environmental, which includes solid debris that disintegrated or decomposed from celestial or man-made materials. Expert views differ as to whether asteroids really pose enough of a problem to develop defenses against the threat.[1] Nevertheless, the threat results from the kinetic energy produced by the projectiles roving through space at rapid velocities. Even the smallest fragments pose a potential threat to IIC and satellite collectors. Other environmental threats include radiation and charged particles which come primarily from the sun. These "space weather" effects may be gradual or instantaneous. These effects are usually difficult to detect until after catastrophic failure.

The last threat area involves people and can be subdivided into two categories: the capture of our people implanted with the microscopic chip and the espionage and defection to the enemy side. All three categories of threats (man-made, environmental, and people) will destroy, disable, or degrade our ability to perform tasks that support our core capability of information dominance.

Countermeasures

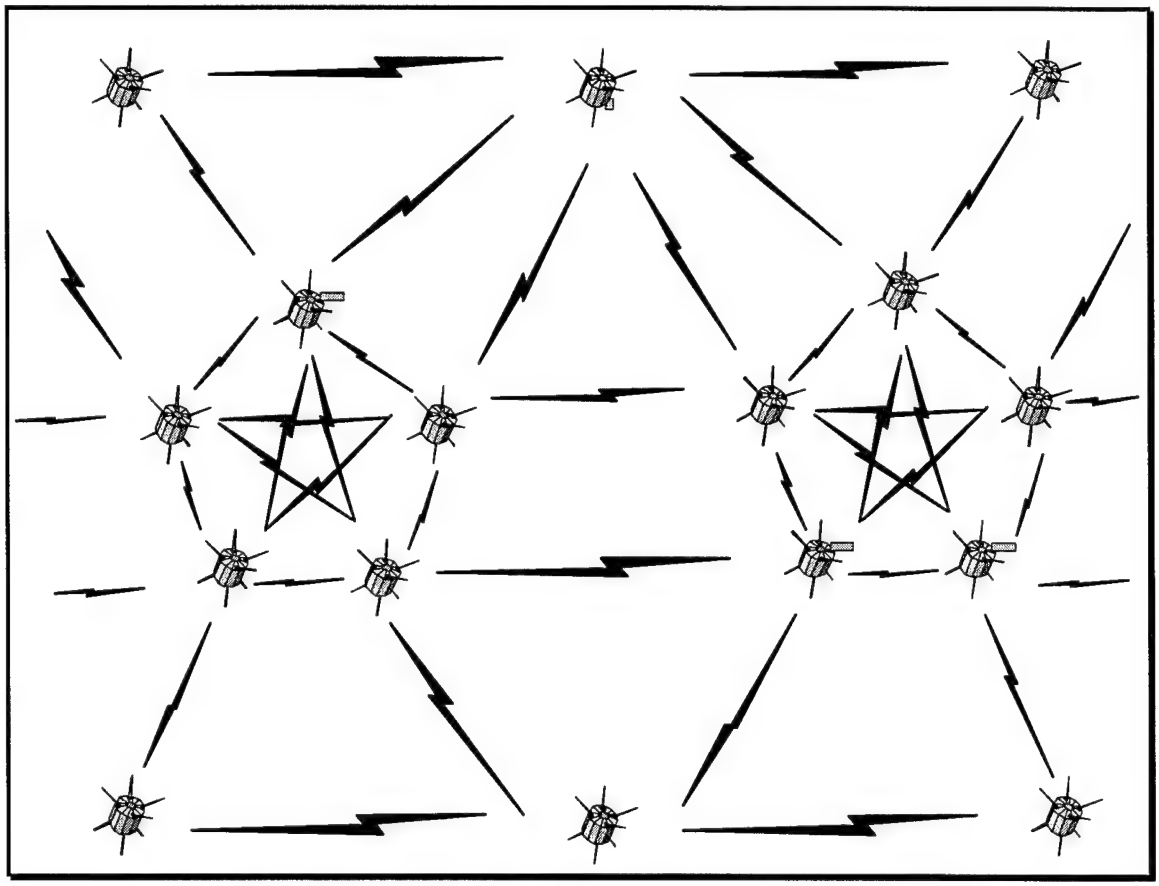
Countermeasures include both passive and active activities that can be used against a variety of threats. The following paragraphs describe several activities and discusses their effect on vulnerabilities.

Distributed System Architecture

The defensive goal behind the use of a distributed system architecture for the IIC is to deny the enemy a center of gravity to attack. In other words, use of this type of architecture will deny the enemy the IIC as a target that if destroyed "would cause a system failure or cascading deterioration within the system," allowing the enemy to achieve its objective.[2]

The network of IIC satellites are interconnected using the "star" interconnectivity, which has lines radiating out from each satellite to other satellites (fig. 5-1).[3] Essentially, the satellite constellation forms a "mesh" over the earth's atmosphere.[4] The interconnected mesh allows for graceful degradation so that if the enemy physically destroys a percentage of the IIC, it does not lead to a total loss of effectiveness. Further,

because of the interconnectivity, the mesh knows to compensate and fill in the gaps created by the destruction. The mesh has no center of gravity so if the adversary wants to defeat the IIC, it must be destroyed in total.[5]



Source: Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

Figure 5-1. Information Integration Center Interconnectivity

The "Small and the Many"

Components that feed information and support the IIC will be composed of many inexpensive sensors, emitters, microsats, and miniprojectiles. Similarly, the IIC mesh also consists of many small satellites (minisats) that are inexpensive and easy to launch. Current minisat development and designs produced satellites that weigh several hundred pounds and measure about three cubic feet. Recent advancements in electronics and miniaturization have given impetus to smallsat concepts that weigh approximately 20 to 30 pounds and are smaller than shoe boxes.[6]

The qualities of redundancy, miniaturization, and low cost will describe future components that make up the IIC. The "small and the many" concept results in a system that is redundant and difficult to completely

destroy.[7] Like the IIC concept, this concept allows the enemy no center of gravity to target, therefore, no single point of failure. Further, even if adversaries destroy a portion of the network, it will still survive and operate.

"Smart" System

Inherent in the IIC system is the built-in capability to fuse, correlate, and, most importantly, *deconflict* contradictory inputs and data points. Therefore, when adversaries attempt information warfare by injecting false statements (syntactic attacks) into the logic tree, the computing system within the IIC will recognize the inconsistencies and deconflict them. The IIC consists of a body of knowledge and an "ability to learn" to know when a possible conclusion is invalid or simply does not make sense. [8] When the IIC detects inconsistencies, it will seek additional data either to validate or invalidate its own conclusions.

If the individual attempts to enter a particular Cyber Situation when the IIC concludes there are invalid resolutions, it will inform the user of the potentially false inputs and its attempt to resolve the data confliction. If the individual desires, the IIC will show the conflicting data and why a possible conclusion is invalid.

Optical Computing

Much research continues in this area of optical networks to transmit, receive, and store information. The technology appears promising and at minimum would seem a plausible radiation defense.[9] The use of optical computing in the IIC (to receive inputs from other collectors and users, to respond to users' requests to develop the Cyber Situation picture, or to task lethal and nonlethal assets) would serve as protection against radiation threats. Radiation attacks systems that use electrons to transmit data. Since optical computing employs photons instead of electrons, these photons render optical computing systems safe from EMP threats.

Low Earth Orbit

Employing the IIC in a low earth orbit (LEO) will minimize exposure to environmental radiations. Compared to other orbits, the LEO naturally is exposed to lower levels of radiation. By contrast, medium orbits have the highest levels of radiation, primarily caused by the Van Allen Radiation Belts, while at the geosynchronous orbit, the radiation level is higher than the low-earth orbit but lower than the medium orbit.[10]

Internal Deactivation

If captured by the enemy, users with the implanted microscopic chip may self-deactivate the chip and render it useless. Further, the chip disintegrates and cannot be extracted by the enemy for reverse engineering or for adversarial reasons.

External Deactivation

When faced with the disturbing events of espionage and defections of friendly users to the enemy side, the IIC is engineered with the capability to deactivate and disintegrate the offender's implanted chips. The highest level commanders within the US military have the authority to access the IIC and order the system to deactivate the defectors' chips the next time they try to activate the Cyber Situation.

"Zap" Attack

"Zap" attack relies on the decision-support technology built into the IIC and its link to space-based laser weapons. As individual satellites within the IIC network sense an object (man-made or environmental) moving toward its network, the IIC will compute the object's directional objective, velocity and acceleration, and Doppler shift to determine whether it is a threat. If the decision is affirmative, the IIC will instruct the nearest space-based laser weapon to destroy the object and eliminate the threat to the IIC system.

"Mutual Dependence"

Once implanted, the microscopic chip will operate only when the individual is alive because the chip creates mutual dependence on its host. In the unfortunate circumstance where a Cyber Situation user dies, the implanted microscopic chip becomes nonfunctional and disintegrates. This operational dependence of the chip upon its host prevents adversaries from using a chip from a deceased war fighter.

Summary

Table 15 presents a list of threat categories and associated countermeasures that will address each type of threat. Note that each countermeasure may be effective against more that one type of threat.

Table 15

Countermeasures Versus Threats

	Threat		
Countermeasure	Man-made	Environmental	Human
Distributed System Architecture	X	X	———
"Small and the Many"	X	X	———
"Smart" System	X	———	X
Optical Computing	X	X	———
Low Earth Orbit	———	X	
Internal Deactivation	———	———	X
External Deactivation	———	———	X
"Zap" Attack	X	X	———
"Mutual Dependence"	X	———	X

Though numerous vulnerabilities exist with the Cyber Situation, by 2025 effective countermeasures likely will be integrated into the system. Well-developed measures to defeat these man-made, environmental, or human threats can make the Cyber Situation more effective to the war fighter. Chapter 6 goes beyond threats and countermeasures and will explore potential structure and doctrine changes required to achieve and take full advantage of the Cyber Situation.

[1] Anonymous assessor comment on 2025 Paper Draft (Maxwell AFB, Ala.: Air War College/2025, 1996).

[2] Paul Moscarelli, *Strategic Structures Course Book*, vol 2, *Operational Analysis: An Overview* (Maxwell AFB, Ala.: Air University Press, 1995), 522–23.

[3] Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1995), 33.

[4] Martin C. Libicki, *The Mesh and the Net* (Washington, D. C.: National Defense University Press, 1994), 3. Libicki defines *mesh* as "the term applied to military applications—points to the holes; as information technology places a finer mesh atop the battlefield, more objects are caught in it."

[5] Ibid., 33.

[6] Air Force Scientific Advisory Board members, review and comments from 2025 Concept Briefings (Maxwell AFB, Ala.: Air War College/2025, 5 February 1996).

[7] Ibid., 19-37.

[8] Negroponte, 154–56.

[9] Vincent W. S. Chan, "All-Optical Networks," *Scientific American* 273, no. 3 (September 1995): 57–58.

[10] Michael J. Muolo, *Space Handbook: Space Analyst's Guide*, vol 2 (Maxwell AFB, Ala.: Air University Press, December 1993), 13–14.

Chapter 6

Concept of Operations

Today's breathtaking technological achievements notwithstanding, developing the concept of operations that incorporate new technologies and organizations to permit effective exploitation of new capabilities is even more critical than acquisition of the technologies themselves.

—James R. Fitzsimonds
Revolutions in Military Affairs

This chapter discusses how the Cyber Situation will be implemented and expound on what capabilities the Cyber Situation offers to future war fighters. Implementing the system will require dramatic changes to our present-day organizational structure and doctrine. No doubt some of these changes will appear radical and meet stiff resistance by individuals and institutions unconvinced of the merits the Cyber Situation has to offer to the defense efforts of United States military. History has shown those entities unable or unwilling to adapt to change have, at best, been left behind, and in the worst instances been eliminated as an entity.

To realize the full potential of the Cyber Situation, tomorrow's aerospace forces must devise dramatically different supporting organizations and doctrine in order to fully harvest these innovative new capabilities. As noted in previous chapters, the technology will be available in 2025; it will be the organization and command structures along with the doctrine and concept of operations (CONOP) that will form the second and third legs of the revolution in military affairs (RMA) triad.

Future Conops

War-fighting and conflict management in 2025 will apply the results of improved concepts and technology applications in the areas of surveillance and reconnaissance, command and control, and overall

battlespace execution. As forecast in the 1994 SPACECAST 2020 study, "advances in surveillance and reconnaissance, particularly real-time 'sensor to shooter' to support 'one shot, one kill' technology, will be a necessity if future conflicts are to be supported by a society conditioned to 'quick wars' with high operational tempos, minimal casualties, and low collateral damage."[1] The Cyber Situation has the potential to be the harbinger of the revolution.

Applications of the Cyber Situation

The Cyber Situation is ideally suited for the command, control, and execution of military operations across the spectrum of warfare from the selective release of nonlethal weapons to the full-scale assault of parallel war. In parallel war, aerospace forces simultaneously attack enemy centers of gravity across all levels of war (strategic, operational, and tactical) at rates faster than the enemy can react.[2]

Commanders always seek to control the throttle of the OODA Loop, operating faster or slowing the decision cycle of their foes. In past wars, tank commanders and fighter pilots always strove to get "inside the enemies OODA Loop." The difference in future conflicts will be the speed and scope of their decisions.

Parallel war requires large numbers of highly precise weapons directed against critical nodes. Additionally, they require a requisite level of detail on the enemy situation necessary for precision targeting. For these reasons yesterday's military commanders could not wage parallel war effectively. The Cyber Situation is ideal for conducting parallel war because it offers capabilities that fill both of these voids.

The Cyber Situation offers tomorrow's commanders an in-time view of the battlespace, exposing the enemy centers of gravity before his eyes. In 2025 operating at previously unheard of speeds will be a common feature of military engagement. Future warriors by way of the IIC will conduct Cyber Situations utilizing a whole new array of air and space sensors, UCAV, directed energy weapons, and highly mobile expeditionary forces. Operations will be controlled from Cyber Situations in continental US (CONUS) and instantaneously reach out and touch the enemy halfway around the globe.

A CONUS-based joint task force commander, for example, would have well exercised connectivity with combat units through Cyber Situations with CONUS-based stealth bombers, UCAV, and instantaneous

access to space based precision strike weapons. Imagine the psychological effect on the adversary who will be unable to predict where the next blow will fall and will be powerless to defend against it

Command Structure

The 2025 force structure and battlespace requirements will make obsolete traditional hierarchical command and control arrangements. Cyber Situation capabilities require greater decentralization through information technology, growth of distributed systems and establishment of virtual organizations.

> New information and communications technologies are shifting power to those with the most powerful computers and most effective sensors . . . at the same time, the punch packed by the individual soldier is increasing, eroding the role of field commanders and resulting in flatter command and control structures.[3]

The Cyber Situation allows greater emphasis to be placed on decisive decision making, precision engagement, high-speed and synchronized maneuver, agility, and enhanced command and control. The command structure will have freedom of operation within previously identified parameters much like the vaunted German decentralized, flexible command style known as *Auftragstaktik* (mission tactics). This method of battlefield command has enabled smaller forces to defeat much larger ones through a timely ability to seize the initiative and act according to "on the spot" judgment. The German breakout at Sedan, resulting in the fall of France in 1940 offers a familiar example of the successful employment of this flexible command philosophy.[4]

The war fighter must have access to a broad range of supporting weapons, improved mobility, survivability, and supportability—these changes that reflect a dramatically flattened command structure staffed by an extremely high caliber individual at every level. As the battlefield becomes less dense and more decentralized, the demands on small unit leaders increase. The flattened structure permits power to be defused and redistributed, often to subordinate actors. The overall impact is that the flow of information, and its associated awareness and knowledge, compels closed systems to open, eliminating many layers of the cumbersome and compartmented intelligence and analysis bureaucracy. The traditional emphasis on command and control will give way to an emphasis on consultation and control. This organizational structure permits the Cyber Situation to operate at maximum efficiency. It allows commanders at all levels to operate with greater latitude and autonomy as part of an integrated joint operation—a truly combined arms.

Principles of War

The Cyber Situation will provide enormously enhanced capabilities and opportunities for the war fighter, but it will not alter the fundamental principles of war--objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity. These nine principles guide war-fighting at all levels of warfare and have withstood the test of time and will endure in 2025 as the bedrock of US military doctrine.[5] The Cyber Situation optimizes the principles of offense, mass, and maneuver, enabling the commander to execute a wide array of precision weapons from CONUS across the spectrum of warfare at a single decisive point or a parallel attack against multiple critical nodes. The following section depicts the Cyber Situation in action in a hypothetical 2025 scenario.

A Future World

(12 March, 2025--1435 EST/2045Z) The persistent flashing blue light at the corner of his vision alerted the CJCS that the NMCC was initiating a category II ALERT, the blue code for International, Domestic. As the chairman made himself comfortable, he double-blinked rapidly to set in motion his Cyber Situation. As his computer-generated mental display command center whirled into being before his eyes, his mental display-mail--the message that started the ALERT--became operational. CINCSOUTH's image appeared and began briefing.

The government of Argentina was asking for help in conducting a hit on a narcoterrorist group hidden within a room in the center of the Zircon building, a 50-story skyscraper building in downtown Buenos Aires. The Argentina government is worried because the building also contains thousands of civilians unaware of the terrorists' presence. A moment's thought and the topographical detail map of Buenos Aires floats into view. As the CJCS studied the map from all angles, zeroing in on the Zircon building, the other major players "stepped" one by one into the "Cyber conference." The NCA, along with the unified CINCs, service chiefs, and State Department representatives all studied the unfolding three-dimensional schematics of the Zircon building within their own personal "cyberspace." Weather reports began to come in, indicating a storm raging off the coast in Tierra Del Fuego with winds NNE at 35 miles per hour. Light rain was falling in and around Buenos Aires. Now the CJCS moved into the "Cyber Situation" of the intelligence analyst that had been monitoring the situation. DNA and heat-sensing probes of the Zircon building were built into a three-dimensional map that pin-pointed the location of the terrorists on the 23rd floor in the offices of the Argentina Spaceways Co. Two floors above, a local telecommunications company was hosting an AT&T International conference. Local police already had sealed off the outer sectors of the building.

After studying the situation, the CINCSOUTH then ordered the execution of Operation Red Ball One--Option 2, with the CJCS approval. At this point the CSAF took over the "Cyber Situation" and entered the "Cyber-space" of the ACC commander. Together, they reviewed the life-like images that appeared before them marking US

Aerospace bases. Beside each image were the unit's designator, manning level, and current activity. For the execution of Red Ball One--Option 2, after consulting his crisis action staff, the ACC commander decided to precision drop three squads of Space Marines from a TC-4 Globemaster on to the roof of the Zircon building. The Cyber Situation now included the colonel in charge of the 3d Special Operations Group the squadron commander of the Space Marines at Hurlburt Field, Florida, and the Globemaster wing commander at Eglin AFB, Florida. Together, they reviewed the prevailing weather conditions, where the wind and rain could affect operations. Next, they reviewed the computer-generated mental display schematics of the Zircon building, deciding where best to precision drop the squads, mapping out the ins and outs of the stairways and speed lifts of the building. Each of the three squad leaders of the Space Marines entered the "Cyber Situation" for a detailed briefing of the Zircon building's many exits and entries. They discussed the placement of portable force-field shields to isolate the floor and at what point the various nonlethal weapons would be used. One of the Marines suggested using an ultra-high frequency wave burst as the best method to subdue the terrorists with the fewest losses. The TAV-4 pilot and crew, already part of the Cyber Situation, once more reviewed the weather, adjusted for winds, and with the squadrons aboard, launched.

The CINC and others watched the outcome of the operation in their "Cyber Situations," noting the success of the precision drop and the excellent execution of the Space Marines in avoiding detection by the terrorists, while keeping the civilians calm. The success of the frequency wave burst earned the suggesting Space Marine a merit promotion and the entire operation the Argentine government's heartfelt thanks.

Notes

[1] SPACECAST 2020, "Leveraging the Infospace: Surveillance and Reconnaissance in 2020" (Maxwell AFB, Ala.: Air University Press, June 1994), 1.

[2] Jeffrey R. Barnett, Future War: An Assessment of Aerospace Campaigns in 2010 (Maxwell AFB, Ala.: Air University Press, 1996), 6.

[3] Institute for National Strategic Studies, *Strategic Assessment 1995: US Security Challenges in Transition* (Washington, D. C.: National Defense University Press, November 1994), 16.

[4] Robert Allan Doughty, *The Breaking Point: Sedan and the Fall of France, 1940* (Hamden, Conn.: Archon Books, 1990), 3.

[5] Joint War-fighting Center Doctrine Division, *War-fighting Vision 2010: A Framework For Change* (Langley AFB, Va.: 1 August 1995), 2.

Chapter 7

Investigation Recommendations

This chapter discusses areas of concerns requiring increased R&D and time investment. First, it articulates specific shortfalls and identifies commercial and military solutions. Second, it identifies broader issues that will develop with the overall implementation of the Cyber Situation.

Some elements of the Cyber Situation have progressed further in the development process than others. By 2025 the communications architecture will be sufficiently robust to support the Cyber Situation. This will occur because of significant commercial investment as the civilian sector's insatiable appetite for increasingly rapid access to data facilitates greater profit for those who provide it. The military will likely be an investment partner in communications advances.

Computer power will continue to progress, doubling about every 18 months until the turn of the century. Again, the commercial sector will take the lead with the military purchasing adequate computer power "off the shelf."

Current development in other areas is not as advanced and will therefore require greater emphasis to mature at a comparable rate. Intelligent software is becoming more commonplace and its application more widely implemented. However, currently available intelligent software has narrow application and is neither very complex nor does it possess suitable capacity. To achieve the military requirements of the Cyber Situation, allocation of R&D funding must continue to increase the pace of development in intelligent software applications.

Finally, 2025 intelligence collection requires technology advances in both computer power and intelligent software but currently is more affected by the developmental limitations in intelligent software. Commercially available intelligence software is proliferating and will augment products developed and

managed by the military. However, development of small satellites, both capable of short duration intelligence gathering as well as the ability to cover communication gaps, will require the infusion of scarce military dollars to supplement private sector investment.

The following are other, broader issues that require attention. First, the developmental technologies required by the Cyber Situation must have a more effective linkage. Since each of the capability areas required by the Cyber Situation is developing on a separate path, the synergistic effect of combining these areas might better achieve the goal of complete OODA integration.

Second, research into the functions of the brain must be encouraged and accelerated. This is a new area for both the medical community and the military. The research effort must focus on the capacity and interface within the brain and how information is processed in going from raw input to final decision.

Third, social and cultural biases to a brain implanted decision tool must be overcome. The Cyber Situation is designed to assist, *not* control each decision maker. To fully exploit growing technology, cumbersome hardware and software requirements must be reduced to the simplicity and seamlessness of a chip implant. With that technology in hand, the Cyber Situation can become a reality.

Chapter 8

Conclusion

The Cyber Situation makes the entire OODA Loop available to the commander in one location. It provides observation through the collection platforms, the IIC, and the computer chip. It orients the user using the IIC, the archival databases, and the brain chip. These are neither new nor revolutionary capabilities provided to the commander. Senior decision makers throughout time have had access to the orient and observe portion of the OODA.

Where the Cyber Situation provides a unique orient and observe capability to the commander is the rapidity in which a decision maker has access to a complete picture. Before the Cyber Situation linked the collectors and analysis tools in one step, each event was accomplished singly. Collectors were tasked and controlled by one group and the analysis occurred elsewhere. The collected and analyzed information then had to be briefed or presented to the commander who applied his own analysis to the information and determine his own solution. This information could (and often did) come to the commander incomplete or with biases attached. The Cyber Situation cuts through the processing and provides the commander with an in-time picture from which he can observe and orient to an unbiased and a complete picture.

With the commander fully informed, the Cyber Situation helps with the decision process. The Cyber Situation is designed to be a *decision aid* not a *decision maker*. This none-too-subtle difference confirms that, as conceived, the capability resident in the Cyber Situation is designed to facilitate the best possible decision from a human, who will always be in the loop. Options available to commanders for any situation will be clearly displayed and evident to them; they can select one or seek additional information from the Cyber Situation before proceeding.

It is in the final area of the OODA Loop, the act, where the Cyber Situation provides true added value. Once the commander has fully observed, oriented, and reached a decision, action can occur. The full impact of this full spectrum of the OODA Loop cannot be over stated.

Prior to the full deployment of the Cyber Situation, even the best complete strategic OODA cycle will continue to take hours or days. Providing the commander with the information needed to reach the point of action meant collecting the right data, putting it in the hands of the right analyst, and providing that information to the commander. This is a cumbersome process at best, often overcome by events before the information was forwarded to the right decision maker. Since there was a time-consuming structure in place, information was unavoidably dated (even the freshest information is minutes old) and often incomplete. Thus, even under the most terrific circumstances, the commander was making a decision and perhaps employing forces without the best information.

Not only was the information incomplete, decision makers often contemplated as to whether the information their subordinates provided was reliable and credible. With the capability provided by the Cyber Situation, the information accuracy will be reliable and credible. Further, decision makers will have unobstructed access to information. In short, a decision can finally be made *with a complete picture of the battle space.*

Once a decision had been reached, the commander transmits execution orders. These orders must be properly formatted and transmitted to subordinate units for action. Again, there is an unavoidable time lag between when the orders are transmitted and when they are acted upon. In these precious hours, the situation the commander desires to effect can change dramatically.

With the capability provided by the Cyber Situation, the commander can employ forces instantly and flexibly. Whether the weapon of choice is a laser, UAV, or F-22, through the Cyber Situation the commander has instant access to it.

What is even more compelling about the capability available through the Cyber Situation is that with the exception of the brain chip, the technologies required to field it are well along in development in 1996. Communications architectures are growing in both commercial and military applications and computer power is still on an exponential growth rate. Software, too, is becoming more intelligent. Indeed, the required capability is on the horizon.

In the end, the development of the Cyber Situation becomes a matter of priorities and trade offs. The question that must be asked at the highest levels in the Department of Defense is whether or not bits are as important as bullets and how the DOD budget dollar must be spent to satisfy the operational requirements for air power in 2025. If what is required is the capability to provide the commander with all the information and tools to act on a decision, then the Cyber Situation is the solution.

Appendix A

List of Acronyms and Abbreviations

ARPA	Advanced Research Project Agency
ACC	Air Combat Command
AOR	area of responsibility
CRT	cathode ray tube
CJCS	chairman, joint chiefs of staff
CSAF	chief of staff, US Air Force
C^4I	command, control, communications, computers, and intelligence
CINC	commander in chief
SOUTHCOM	commander in chief, Southern Command
CONUS	continental United States
DNA	deoxyribonucleic acid
DOD	Department of Defense
DSB	direct satellite broadcast
EEG	electroencephalograph
EMP	electromagnetic pulse
GII	Global Information Infrastructure
HCI	human computer interaction
IU	image understanding
IIC	Information Integration Center
I3	intelligent integration of information
JTF	joint task forces
MII	Military Information Infrastructure
MLS	multilevel security
NCA	National Command Authority
NII	National Information Infrastructure

NMCC	National Military Command Center
NWV	New World Vistas
OODA	observe, orient, decide, and act
PDA	planning and decision aids
R&D	research and development
RMA	revolution in military affairs
TAV	transatomospheric vehicle
UAV	uninhabited aerial vehicles
UCAV	uninhabited combat aerospace vehicles
URAV	uninhabited reconnaissance aerospace vehicles

Bibliography

Advanced Projects Research Agency. *Intelligent Systems.* On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Intel_Thrust.html.

Advanced Projects Research Agency. *The SISTO Solution: Intelligent Software Systems.* On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Solution.hmtl.

AFM 1-1. *Basic Aerospace Doctrine of the United States Air Force. 2 vols.,* March 1992.

2025 Concept, No. 200169. 2025 Concept Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900272, "Very High Altitude Balloon-Borne Systems,. 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900280, "Fly on the Wall." No. 900434, "Airborne Sound Sensors." 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900438, "Ultraendurance High-Altitude Ocean Loitering Uninhabited Reconnaissance Vehicle." 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900517, "JSTARS Replacement." 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900552, "On-demand Tactical Recce Satellite Constellation." 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900604, "UAV Constellations," 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

2025 Concept, No. 900702, "Implanted Tactical Information Display." 2025 Concepts Database Maxwell AFB, Ala.: Air War College/2025, 1996.

Air Force Executive Guidance (draft), HQ USAF/XOXS, December 1995.

Amato, Ivan. "Animating the Material World." *Science* 225 (17 January 1996).

Anonymous assessor comment on 2025 Concept, No 900702. 2025 Concept Database. Maxwell AFB, Ala.: Air War College/2025, 1996.

Anonymous assessor comment on 2025 Paper Review Maxwell AFB, Ala.: Air War College/2025, 1996.

Army Space Institute. "Space Support in Mid-Intensity Conflict." In *Theater Air Campaign Studies Course Book.* Vol. 8. Maxwell AFB, Ala.: Air University Press, 1995.

Baird, Lt Col Henry, et al. "Spacelift." 2025 White Paper. Air University, Maxwell AFB, Ala., April 1996.

Barnett, Jeffery R. *Future War*: *An Assessment of Aerospace Campaigns in 2010.* Maxwell AFB, Ala.: Air University Press, 1996.

Bass, Thomas A. "Gene Genie." *Wired,* August 95.

Carmichael, Lt Col Bruce, et al. "STRIKESTAR 2025." 2025 White Paper. Air University, Maxwell AFB, Ala., April 1996.

Chan, Vincent W. S. "All-Optical Networks." *Scientific American* 273, no. 3 (September 1995).

Clinton, William J. *A National Security Strategy of Engagement and Enlargement.* Washington, D. C.: The White House, February 1996.

Doughty, Robert Allan. *The Breaking Point: Sedan and the Fall of France, 1940.* Hamden, Conn.: Archon Books, 1990.

Electronics Visualization Laboratory, University of Chicago at Illinois (No date). *The CAVE: A Virtual Reality Theater.* On-line, internet, no date, available on http://www.ncsa.uiuc.deu/EVL/docs/html/CAVE.html.

Engelbrecht, Col Joseph A. 2025 Research Director, and Professor of Conflict and Change, Air War College. Maxwell AFB, Ala. Personal interview by Maj YuLin Whitehead, 17 April 1996.

Firschein, Oscar, and Thomas Strat *Image Understanding Program.* On-line, internet, 23 July 1995, available on http://www.arpa.mil/sisto/Overview/Image.html.

Fitzsimonds, James R., and Jan M. Van Tol. "Revolutions in Military Affairs." *Joint Forces Quarterly*, no. 4 (Spring 1994).

Fogleman, Gen Ronald, lecture to 2025 participants. Air University. Maxwell AFB, Ala., 13 February 1996.

Fukuyama, Francis. RAND Corporation, Washington D. C. Electronic mail. Subject: Dross and Gold, 27 December 1995. Used by permission of author.

Garvey, Dr Tom . *Planning and Decision Aids Program.* On-line, internet, 23 July 1995, available from on http://www.arpa.mil/sisto/PDA.html.

Grier, Peter. "New World Vistas." *Air Force Magazine* 79, no. 3 (March 1993).

Gunning, David. *Intelligent Integration of Information (I3).* On-line, internet, 23 July 1995, available from on http://www.arpa.mil/sisto/I3.html.

Institute for National Strategic Studies. *Strategic Assessment 1995: US Security Challenges in Transition.* Washington, D. C.: National Defense University Press, November 1994.

Jefts, Maj Barbara, et al. "Virtual Integrated Planning and Execution Resources System: The High Ground of 2025." 2025 White Paper, Air University, Maxwell AFB, Ala., April 1996.

Joint War-fighting Center, Doctrine Division. *War-fighting Vision 2010: A Framework For Change.* Langley AFB, Va.: 1 August 1995.

Kalmanek, Charles, and K. G. Ramakrishnan. "On-line Routing for Virtual Private Networks" (Paper presented at the Third International Telecommunications Symposium, September 1995). On-line, internet, September 1995, available on http://www.research.att.com/hgs/infocom95/program.html.

Kolarov, Aleksandar, and Joseph Hui. "Least Cost Routing in Multiple-Service Networks: Part II" (Paper presented at the Third International Telecommunications Symposium, September 1995). On-line, internet, September 1995, available on http://www.research.att.com/hgs/infocom95/program.html.

Krepinevich, Andrew F., Jr. "The Military-Technical Revolution: A Preliminary Assessment." In *War Theory Course Book.* Vol. 3. Maxwell AFB, Ala.: Air University Press, September 1995.

Libicki, Martin C. *The Mesh and the Net: Speculation on Armed Conflict in a Time of Free Silicon.* Washington, D. C.: National Defense University Press, 1994.

McGinnis, Lt Col Michael L., and Maj George F. Stone III, "Decision Support Technology." *Military Review* 74, no. 11 (November 1994).

McKitrick, Jeffrey, et al., "The Revolution in Military Affairs." In *Air War College Studies in National Security: Battlefield of the Future.* No. 3. Maxwell AFB, Ala.: Air University Press, September 1995.

McMillan, Lt Col James. Air Force Liaison to National Security Agency. Telephone interview by Maj Scott Bethel, 26 February 1996.

Moscarelli, Paul. "Operational Analysis: An Overview," In *Strategic Structures Course Book.* Vol. 2. Maxwell AFB, Ala.: Air University Press, 1995.

Muolo, Maj Michael J. *Space Handbook; An Analyst's Guide.* Maxwell AFB: Air University Press, 1993.

Negroponte, Nicholas. *Being Digital.* New York: Vintage Books, 1995.

Norman, Maj Cindy, et al. "Man In the Chair." 2025 White Paper, Air University, Maxwell AFB, Ala., April 1996.

Patterson, David A. "Microprocessors in 2020." *Scientific American* 273, no. 3 (September 1995).

Petroski, Henry. *To Engineer is Human.* Chicago: University of Chicago Press, 1989.

Psaltis, Demetri, and Fai Mok, "Holographic Memories," *Scientific American* 273, no. 5 (November 1995).

Robinson, Clarence A. "Molecular Biology Computation Captures International Research," *Signal* 50, no. 6 (February 1996).

Rogers, Craig A. "Intelligent Materials." *Scientific American* 273, no. 3 (September 1995).

Sawyer, Ralph D. *The Seven Military Classics of Ancient China.* Boulder, Colorado: Westview Press, 1993.

Scientific Advisory Board members, Comments from 2025 Concept Briefings Maxwell AFB, Ala., February 5, 1996.

Sears, Allen, and Robert Neches. *Human Computer Interaction Program.* On-line, internet, 23 July 1995, available on http://www.arpa.mil/sisto/HCI.html.

Sherman, Bill. *NCSA Virtual Reality Lab & CAVE.* On-line, internet, 18 February 1996, available *on* http://www.ncsa.uiuc.edu/VR/VR/.

Simon, Herbert A. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization.* 3d Ed. New York: The Free Press, 1976.

Simonsen, Maj Philip, et al. "SPACENET: ON-ORBIT SUPPORT IN 2025." 2025 White Paper. Air University, Maxwell AFB, Ala., April 1996.

SPACECAST 2020. "Leveraging the Infospace: Surveillance and Reconnaissance in 2020," SPACECAST 2020. Vol. 1. Maxwell AFB, Ala.: Air University Press, June 1994.

Szafranski, Col Richard, and Col Joseph A. Engelbrecht, Jr. "The Structure of the Revolution: Demystifying the RMA." Unpublished paper, March 1996.

Takano, Makoto, and Katsumi Fujita. "Multilevel Network Management by Means of System Identification" (Paper presented at the Third International Telecommunications Symposium, September 1995). On-line, internet, September 1995 , available on http://www.research.att.com/hgs/ infocom95/program.html.

Thomas, Peter. "Thought Control," *New Scientist* 149, no. 2020 (9 March 1996).

Tiernan, Maj Mike, et al. "In-Time Information Integration System." 2025 White Paper. Air University, Maxwell AFB, Ala., April 1996.

Toffler, Alvin and Heidi Toffler. *War and Anti War.* New York: Warner Books, 1993.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century.* Unpublished draft, the Human Systems and Biotechnology Volume. 15 December 1995.

———. *New World Vistas: Air and Space Power for the 21st Century.* Unpublished draft, the Information Applications Volume. 15 December 1995.

———. *New World Vistas: Air and Space Power for the 21st Century.* Unpublished draft, the Information Technology Volume. 15 December 1995.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century,* Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

Vincent, 1 Lt Gary A. "In the Loop: Superiority in Command and Control." In *Operational Structures Course Book.* Vol. 5. Maxwell AFB, Ala.: Air University Press, November 1995.

Westenhoff, Charles M., ed., *Military Air Power.* Maxwell AFB, Ala.: Air University Press, 1990.

Widnall, Dr Sheila E. and Gen Ronald R. Fogelman, *Air Force Executive Guidance.* Washington D.C., December 1995.

———*Cornerstones of Information Warfare.* Washington D.C., 1995.

Zysman, George I. "Wireless Networks." *Scientific American* 273, no. 3 (September 1995).